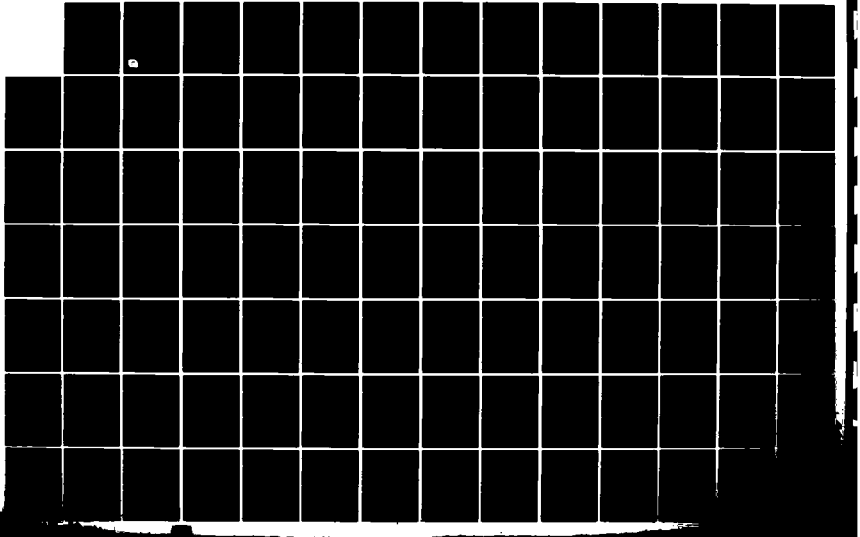
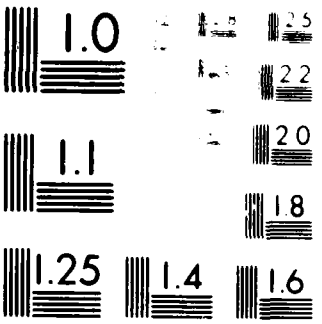
AD-A149 876 COMPUTER ABUSE AND MISUSE: AN ASSESSMENT OF FEDERAL AND STATE LEGISLATIVE..(U) INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA L G BECKER DEC 84 IDA-P-1798 1/2

UNCLASSIFIED IDA/HQ-84-29067 MDA903-84-C-0031 F/G 9/2 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS

Copy 88 of 130 copies

AD-A149 876

(2)

IDA PAPER P-1798

COMPUTER ABUSE AND MISUSE: AN ASSESSMENT OF FEDERAL AND STATE LEGISLATIVE INITIATIVES

Louise Giovane Becker

December 1984

DTIC ELECTE FEB 8 1985 S D B

DTIC FILE COPY

Prepared for

The Assistant Secretary of Defense
(Command, Control, Communications and Intelligence) C^3I

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

INSTITUTE FOR DEFENSE ANALYSES

IDA Log No. HQ 84-29067

The work reported in this document was conducted under Contract No. MDA 903 84 C 0031 for the Department of Defense. The publication of this IDA Paper does not indicate endorsement by the Department of Defense nor should the contents be construed as reflecting the official position of that agency.

This paper has been reviewed by IDA to assure that it meets high standards of thoroughness, objectivity, and sound analytical methodology and that the conclusions stem from the methodology. IDA does not, however, necessarily endorse the conclusions or recommendations that it may contain.

Approved for public release; unlimited distribution.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD A149676	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Computer Abuse and Misuse: An Assessment of Federal and State Legislative Initiatives		5. TYPE OF REPORT & PERIOD COVERED FINAL - July - Dec 1984
		6. PERFORMING ORG. REPORT NUMBER IDA Paper P-1798
7. AUTHOR(s) Louise Giovane Becker		8. CONTRACT OR GRANT NUMBER(s) MDA 903 84 C 0031
9. PERFORMING ORGANIZATION NAME AND ADDRESS Institute for Defense Analyses 1801 N. Beauregard Street Alexandria, Virginia 22311		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Task T-4-253
11. CONTROLLING OFFICE NAME AND ADDRESS Assistant Secretary of Defense (C^3I) The Pentagon, Room 3E172 Washington, D.C. 20301		12. REPORT DATE December 1984
		13. NUMBER OF PAGES 165
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) DoD-IDA Management Office 1801 N. Beauregard Street Alexandria, Virginia 22311		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE NA

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; unlimited distribution.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

computer abuse, computer security, computer crime legislation and statutes, automated information systems security

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The importance of computer-related resources to the management and analysis of DoD operations prompts consideration of legal and administrative measures to improve the security posture of automated information systems. Incidents of computer abuse and misuse continue to receive national attention. Most recently two distinct events, the issuing of the National Policy on Telecommunications and Automated Information Systems Security (NSDD-145) and (continued)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

20. Continued

the enactment of a Federal computer crime statute, give new impetus to examining of key issues. These issues include the possible expansion of Federal jurisdiction, scope of computer abuse, definitional problems within the legislation, and the need for additional statutory language. This paper includes a review of current Federal legislative measures and selected State statutes. Highlighted are the implications for DoD and the challenge of developing adequate legal and administrative means to combat computer abuse. An important set of conclusions is that attention is needed to improve computer security technologies to monitor and prevent abuses, improve the capability of investigators and others to detect abuses and collect evidence, reduce the technology gap, and raise awareness of the potential for computer abuse.

IDA PAPER P-1798

COMPUTER ABUSE AND MISUSE: AN ASSESSMENT OF FEDERAL AND STATE LEGISLATIVE INITIATIVES

Louise Giovane Becker

December 1984

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311

Contract No. MDA 903 84 C 0031
Task T-4-253

PREFACE

This paper was prepared for the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) C^3I. It is designed to provide a framework for understanding the technical aspects of computer abuse legislative initiatives. The focus is on the recently enacted Federal computer crime statute, some of the pending Federal bills, and selected state computer crime statutes. The ramifications of the legal remedies to combat computer abuse and some of the implications for the Department of Defense are addressed herein.

This examination gives an overview of state statutes and the Federal legislation and outlines some of the key issues and legal aspects related to computer abuse and misuse. Chapter I, Overview of Computer Abuse Issues, describes the nature and scope of the problems and highlights the key issues as well as selected Federal initiatives and the recent American Bar Association's computer crime report; Chapter II, Federal Legislative Actions, highlights congressional activity and reviews pertinent Federal legislative measures; Chapter III, State Computer Abuse Statutes, describes some of the state statutes on computer crime and briefly discusses the experiences in enforcement of the law at the state level; and Chapter IV, Directions and Options, addresses some of the implications of computer abuse and misuse for the Department of Defense and recommends certain actions.

The following appendices are also included: a computer-related crime glossary, a bibliography on the subject, full text of selected Federal legislative measures, summary of the American Bar Association (ABA) Report on computer crime, and the text of the unclassified version of the NSDD-145, National Policy on Telecommunications and Automated Information Systems Security.

ACKNOWLEDGEMENTS

The author is indebted to a great number of individuals from government and the private sector who have helped in identification of issues and problems related to computer abuse. Both the policy and technical review process was assisted by the contributions of Alexander Roth (Attorney), David Bailey (Los Alamos National Laboratories), and Richard Van Atta (IDA, Science and Technology Division). Betty Henderson and Joyce Walker provided typing support. The paper was also reviewed by Col. John Lane and Maj. Susan Swift of the Office of the Assistant Secretary of Defense C^3I and by Thomas Probert, Director, IDA, Computer and Software Engineering Division.

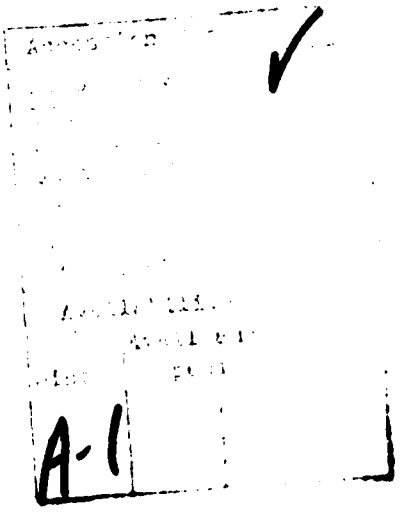


TABLE OF CONTENTS

APPENDICES:

Executive Summary

At the request of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, (C^3I) the Institute for Defense Analyses (IDA) prepared a paper on computer abuse issues and related legislative measures.

Within the Department of Defense (DoD) computer-related resources continue to have an important role. The increased reliance on automated information systems, especially communications network-dependent systems, prompts interest in legal remedies to combat threats to these resources. Traditionally, national security classified data has been the focus of safeguarding efforts. The value of other sensitive data (e.g., financial, inventory, embedded systems) and the proliferation of information technologies prompts consideration of legal and administrative measures to safeguard these resources. The recently enacted Federal "computer crime" statute (P.L. (Public Law) 98-473) and the issuance of the National Security Decision Directive-145 (NSDD-145), "National Policy on Telecommunications and Automated Information Systems Security," provide a new focus for the protection of sensitive information.

The increased dependence on computer-related resources is reflected in the following trends:

- o DoD long-range plans indicate that 75% of technologies being contemplated have an important or essential computer component;
- o Valuable and sensitive data (e.g. financial, inventory, personal, manpower requirements, logistics) are being processed on network-dependent automated information systems;
- o More communications network systems are being implemented; and
- o "User friendly" systems which facilitate access are being developed and employed.

Incidents of computer crime continue to receive national attention but the exact number of incidents of computer abuse is not known. Three factors contribute to the increase in computer abuses:

- o greater access to information technologies and associated resources;
- o dependence on computerized resources to process sensitive and valuable data; and
- o greater number of knowledgeable users.

The Federal computer crime measure, "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" (in P.L. 98-473), is a first step at the national level to provide a specific statutory language to combat computer abuse. The new Act, hastily agreed to in the closing days of the 98th Congress, does not address all of the key concerns. House and Senate conferees agreed to examine other aspects of the issue in the new congressional session. Another key issue has been the benefits of a new

law versus amending of existing statutes. There may be a need to amend both the new law and other existing statutes to provide an adequate set of legal remedies to combat computer-related abuses.

Many of the Federal bills and State statutes evolved from the initial legislation proposed in the late 1970s by then Senator Abraham Ribicoff. Over the years there have been attempts to refine the concepts and identify other issues. Over ten computer abuse bills were considered in the 98th Congress. At the State level over 30 computer crime statutes have been enacted and several bills are pending in State legislatures. These computer crime statutes are designed to protect against a variety of criminal activities and abusive actions involving computers. Both at the Federal and State level, experiences with the new laws are limited, nevertheless, there is some indication that additional statutory language may be needed. Some states are considering amending their computer crime law to reflect the evolution of the technology and the nature of computer abuse.

From this study of the legislative framework it is clear that a number of options should be examined. At this juncture it may be appropriate to consider:

- o <u>assessing the specific dangers to the DoD automated information systems from computer abuse and misuse;</u>

- identifying the capability of DoD to cope with the problem;

- establishing an "early warning" system to identify potential abuses of new information technology;

- encouraging development and implementation of hardware and software features that monitor and control undesired actions; and

- improving training and increasing awareness of the DoD managers and enforcement officials to cope with computer abuse.

CHAPTER I. OVERVIEW OF COMPUTER ABUSE ISSUES

The Department of Defense (DoD) is dependent on a wide spectrum of information technologies, including computer systems, associated communication networks, and related technologies. These systems, while valuable resources in themselves, store and process data critical to the management and analysis of DoD operations and programs. These data clearly should not be vulnerable to compromise or misuse. The need to protect computers and related data from abuse and misuse fosters an assessment of current initiatives to draft computer abuse legislation. This paper examines computer crime and abuse issues and assesses the technological aspects of Federal laws and bills as well as selected state statutes.

DoD has a long tradition of protecting information, especially national security classified data. In addition, special categories of data (e.g. census, tax, personal data, financial records), are protected by Federal statutes. Increased dependence on computers for processing critical and valuable unclassified data prompts interest in effective legal remedies to combat abuse and misuse.

A. NATURE AND SCOPE OF THE PROBLEM

Computer crime and abuse identifies the broad range of intentional acts involving information technologies. These acts may involve "criminal activities directed against computers and their components, criminal activities which use computers or their components as instruments to perpetrate crime, other activities involving computers which, while they may not constitute crimes in the strict legal sense, nevertheless amount to abuse which should perhaps be declared illegal"[1]. Computer crime can be viewed as falling into four major categories[2]:

- Financial Fraud and Theft
- Information Fraud and Theft
- Theft of Services
- Vandalism or Sabotage

Factors that increase the vulnerability of computer-related resources include:

> undesired actions by authorized and unauthorized individuals;
>
> theft of data, services, software and hardware;
>
> lack of appropriate technical safeguards, such as poor management of passwords or lack of encryption;
>
> proliferation of computers, especially those accessible by networks;

increase in number of knowledgeable users; and

certain technical innovations which give unauthorized access.

Computer abuse includes a broader range of actions which may result in unwanted disclosure, denial of services, and destruction of information. Abusive activity ranges from benign disclosure or interception to manipulation and destruction of the information and damage to the associated technologies.

1. Dimensions of Computer Crime

Incidents of computer abuse continue to receive national attention but pinpointing the actual number of transgressions is difficult. Many computer-related offenses are believed to go undetected and those that are uncovered may not always be publicly reported. Many organizations believe that public confidence and trust will be harmed as a result of reporting of a computer abuse. The low probability of detecting a computer abuse coupled with reluctance to acknowledge or publicly disclose incidents makes it difficult to assess the extent of computer abuse activities. Expert witnesses at various congressional hearings and the American Bar Association (ABA) report on computer crime, discussed below, indicate that there is little effort being made to collect information on incidents of abuse. While both the ABA survey and recent media reports seem to

indicate an increase in computer abuse, few reliable assessments of the phenomena are available. The level of abuse within DoD remains largely unknown and a review may be warranted in order to gain a better perspective on the subject.

It is apparent that a relationship exists between the increased accessibility of computer-related resources and the potential for abusing those assets. The problem is often exacerbated by the lack of effective computer security programs. In general, organizations often fail to allocate appropriate resources and order priorities in safeguarding computer-related resources. Since computer security is not without costs many managers attempt to avoid the added expense by ignoring the problems. The lack of appropriate computer security tools contributes to the dilemma. Nevertheless, these factors alone do not fully explain the lack of attention by decision-makers to computer security problems - especially given the fact that in many instances common sense measures may give excellent protection to computer-related resources. For example, changing passwords, establishing administrative safeguards, and instituting good physical security practices provide protection at reasonably low costs.

Another feature that distinguishes computer abuse from traditional crime is that computer abuse may result in very large dollar losses. In a recent congressional hearing it was reported

that losses per incident of computer crime were increasing dramatically. Incidents of extreme dollar losses are illustrated in the following table[3]:

o	1980	$1.2 million	The largest funds transfer fraud.
o	1980	257 people killed	One of the worst airliner crashes caused by criminal negligence in programming a flight navigation computer.
o	1981	$21.3 million	The largest bank embezzlement.
o	1981	$53 million	The largest security fraud.
o	1981	$50 million	The largest commodity fraud.
o	1982	$67 million	The largest inventory fraud.

2. Technological Dimension

Computer abuse is influenced by the rapid evolution of information technology. The wide range of computer appplications processing sensitive data increases the opportunity for abuse and misuse. The importance of computer technology in a modern society, and within DoD, makes it essential to consider an effective approach in safeguarding these resources.

A serious technological gap exists between rapidly evolving information technologies and computer security technology. Development of computer security technologies is currently lagging behind data processing technology. Moreover, in the ABA

report, dicussed below, it was reported that this lag seems to be increasing[4]. This lag in computer security technology development and implementation is believed to contribute in part to increasing opportunities for computer abuse. Manufacturers may fail to close this gap unless there are appropriate incentives. Factors that stimulate computer security technology development deserve further pursuit. The current efforts within DoD, such as the DoD Computer Security Center's program, to develop "trusted systems" deserve additional investment. The focus provided in the National Security Decision Directive-145 (NSDD-145) "National Policy for Telecommunications and Automated Information Systems Security," holds some promise in remedying the situation. That unprecedented new policy presents an opportunity to effectively tackle the computer security technology lag by expanded investment in research and development of computer security technology.

Two other factors that may stimulate the narrowing of the current technology gap include:

1) insurance requirements and

2) demands of the outside auditors for better controls.

These factors will undoubtedly bring pressure on manufacturers to improve security aspects of products to meet new

requirements. Legal liability concerns, insurance requirements, and accountability factors may prove to be important forces in driving the development of computer security technology. New demands for "secure" or "trusted" products stimulated by both Federal and private sector requirements should encourage the market place. For example, the demand for secure products may arise from auditors who require audit trails and other technical protective measures before they certify accounts. Consequently, an essential goal is to encourage the development of computer security products in order to meet current and future requirements.

In congressional testimony it has been suggested that there is a need for a system of "certified products" so that both government and non-government organizations could select the appropriate array of devices to safeguard computers and associated resources. In additional, it has been suggested that there be established a Federally chartered but independent institute to encourage the advancement of computer security technology. This institute, as proposed, would support private sector development and use of computer security innovations.

Additional approachs may be needed to improve both development and implementation of computer security technologies. Consideration should be given to development of appropriate

"prctotypes" or "implementation models" which foster application of advanced computer security technologies.

Another problem, previously referred to, is the reluctance to use existing computer security tools. Innovations, such as commercially available encryption devices, reportedly, are not being universally used.

Unfortunately organizations have a tendancy to ignore computer security problems until faced with a disaster or specific incident. Another factor which makes an organization ignore computer security is the initial cost and the possibility of a decrease in systems performance due to security technologies inefficiency. The development of efficient computer security devices will increase acceptance of these new tools and may ultimately contribute to improving the security of automated information systems.

3. Current Legal Framework

Existing criminal laws, at both Federal and state levels are used to prosecute incidents of computer abuse. More than half the States currently have specific computer crime statutes. Nevertheless, there is a continuing reliance at the State level on criminal statutes such as laws on arson, burglary, larceny, theft of trade secrets, embezzlement, stolen property, forgery,

and anti-tampering to prosecute incidents of computer abuses. While there is now a Federal computer crime statute (P.L. (Public Law) 98-473), the laws invoked in the past to counter computer abuse included those prohibiting arson, embezzlement, theft in interstate and foreign commerce, mail fraud, and interception of wire or oral communications. A number of Federal privacy and computer security statutes have the potential to combat computer abuse; some of these are identified in Figure 1.

It has been suggested that certain statutes (e.g., the Wiretapping Act and the Communications Act of 1934), that control the interception and retransmission of certain communications, if strengthened, will also protect against illegal interception of data and satellite transmissions. Congressional testimony has suggested that these laws be amended to cope with the threat of abuse.

Figure 1

Federal Statutes and Executive Orders applicable to privacy and security aspects of computer-related crime

Citation	Records Affected	Title of Statute
5 U.S.C. 552	G	Freedom of Information Act
5 U.S.C. 552a	G	The Privacy Act of 1974
12 U.S.C. 3401 et seq.	P	Right to Financial Privacy Act
13 U.S.C. 9214	G	Census Act
15 U.S.C. 1666a	P	Fair Credit Billing Act
15 U.S.C. 1681	P	Fair Credit Reporting Act
15 U.S.C. 1693	P	Electronic Funds Transfer Act
18 U.S.C. 641	G	Embezzlement and Theft Prohibition
18 U.S.C. 793, 794	G	Espionage Acts
18 U.S.C. 1343	G-P	Wire Fraud Prohibition
18 U.S.C. 1905	G	Trade Secrets Act
20 U.S.C. 1232g	P	Family Educational Rights and Privacy Act
26 U.S.C. 6103	G-P	Internal Revenue Code on Confidentiality
26 U.S.C. 7609	P	Special Procedures for Third Party Summons
42 U.S.C. 408(h)	G	Confidentiality of Social Security Numbers
42 U.S.C. 5103(b)(2)(e)	G	Confidentiality of Child Abuse Information
44 U.S.C. 3101-3315	G	Records Management by Federal Agencies
44 U.S.C. 3508	G	Interagency Information Exchanges
E.O. 10865	G	Safeguarding Classified Information Within Industry
E.O. 12065	G	Rules Governing Classified Information

Key: G = Government Records Covered
P = Private-Sector Records Covered

Source: U.S. Department of Justice, Bureau of Justice Statistics Computer Crime Legislative Resource Manual. 1980.

4. Increasing Awareness and Improving Education

The lack of information on the scope and nature of computer abuse serves to limit the development of an appropriate computer security program. To improve awareness of the problem and the available safeguards Congress enacted the Small Business Computer Security and Education Act of 1984 (P.L. 98-362). Although the Act focuses strickly on the small business community, its attempt to raise the level of awareness on computer abuse may serve as a model in educating both Federal and private sector decision makers.

The need to protect Federal computerized resources is inherent in a number of government computer resources management statutes such as the Paperwork Reduction Act of 1980 (P.L. 96-511), and Brooks Act, (P.L. 89-306). Additional statutory language which fosters good management practices related to computer resources may be required. There may be a need for specific legislation that would support improved training of computer designers, users, and managers as well as enforcement officials.

B. MAJOR ISSUES

Public debate on computer abuse and misuse centers attention on five key issues:

- o Should Federal jurisdiction be expanded?
- o What is the scope of the computer crime problem?
- o How can definitional problems be resolved?
- o Is there a need for additional Federal computer crime legislation?
- o What new issues require further assessment?

1. Should Federal Jurisdiction be Expanded?

Concerns have been voiced that a national computer crime statute might extend Federal jurisdiction into areas currently handled by state laws. Some of the pending Federal bills seemingly expand government's interest by including Federal computer systems and all those which use "interstate facilities" (e.g., communication networks). Bills containing this language have been interpreted as extending Federal oversight to computer systems currently outside of Federal jurisdiction. Some of the bills currently before Congress extend to all computers that use a common carrier network such as the telephone systems. For example, these bills would apply even when a home personal computer is linked via the telephone system to other computers. Consequently, use of the telephone network in these cases would make such computers subject to Federal oversight.

The expansion of Federal jurisdiction into "computer abuse" is viewed by some as preempting state law and shifting responsibility from the States to the Federal government. This concern

was specifically expressed by Senator Paul Laxalt at the Senate Committee on Judiciary's hearings in 1980 on the "Ribicoff Bill" (96th Congress - S.240). Senator Laxalt emphasized that the bill as drafted would add a new substantive set of offenses to the Criminal Code. He argued that it would also "expand Federal criminal jurisdiction in such a way that the wire and mail fraud statutes pale by comparison[5]." The Administration Bill, S.2940, addresses this problem by narrowing Federal jurisdiction. Specifically, the Adminstration Bill relates to Federal computers, those of financial institutions and those specifically involved from one State to another or from a State to a foreign country, but eliminates the broad language of other pending bills which related to all "computers using a facility of interstate commerce". The elimination of this broad language in the newly enacted Federal computer crime law has prompted Senate and House conferees to agree to consider this matter in the next Congress.

2. What is the Scope of Computer Abuse?

The limited experience with both the Federal and the states' computer crime legislation contributes in part to the incomplete appreciation of the subject. Since computer crime is a relatively new aspect of white collar crime, there has been limited experience in prosecuting the "computer criminal". Moreover, reporting of such crimes is not complete. Incidents of computer abuse often are discovered as a result of accidents.

This factor coupled by a reluctance on the part of victims to disclose incidents of illegal accesses or actual losses, compounds the problem of accurately assessing the scope of computer abuse.

Collecting data on computer crime incidents remains difficult for other reasons. For example, current Federal Bureau of Investigation (FBI) policy calls for categorizing incidents of criminal activity by statute or program, rather than by type of incidents. Computer abuses are not always accurately reported at the State level. Consequently, very little hard statistical data on the dimensions of computer-related crime is known. In part this lack of information on the subject is fostered by the view that the computer is an instrument of some other form of traditional crime, for instance, theft or larceny. In testimony before Congress, the FBI explained that in their view a computer is much like a "gun, a knife or a forger's pen"[6] in that it aids the computer criminal to commit a traditional crime (e.g. fraud, or embezzlement). This perspective and the limited experience with the computer crime statute contribute to a lack of understanding of the extent of computer abuse.

Currently two initiatives are being taken to obtain better information on the dimension of computer crime in the Federal Government:

(1) The Department of Justice has established a Fraud And Corruption Tracking System (FACTS). This recently initiated system provide information on incidents of Federal computer crime.

(2) The Presidents Council on Integrity and Efficiency (PCIE) conducted an initial survey on Computer Crime. The results were reported in Computer Related Fraud and Abuse in Government Agencies. A second follow up survey is being considered.

Recent media reports, for example, focus attention on the "computer hacker" (the unauthorized individual who access an automated information system). A "computer hacker" generally refers to someone with intense interest in exploring the capabilities of computers and communications systems. "Computer-hackers" are responsible for a wide spectrum of activity from benign to malicious. "Hackers" have been known to destroy or contaminate files or obtain access to simply use a computerized resource. Recent reports of intrusions into the TRW credit record systems, the NASA Marshall Space Flight Center as well as penetrations by the "414" Milwaukee based group of teenagers into the Los Alamos National Laboratory and other systems have centered attention on the "hackers". Testimony before both House and Senate Committees and the media indicate that "computer hackers" gain access, manipulate files, use services, and

sometimes damage and destroy files. These incidents, in the judgement of some experts, are "just the tip of the problem". They believe that many intrusions go undetected as well as unreported. Nevertheless the "computer hacker" has focused attention on a generic problem of the unauthorized and the unwanted intrusion into an automated information system.

How serious the threat is from the "computer hacker" continues to be debated. In the opinion of computer security expert Robert L. Courtney, the importance of the "computer hacker" does not rank high. In testimony before a Senate Panel he commented that[7]:

> I think the depredations of kids on terminals playing games, I would have to rank in dollar importance after leaky roofs and overflowing lavatories in their impact on data processing shops.

Nevertheless, both authorized and unauthorized individuals may access systems to destroy, manipulate, or compromise computer related resources. In the opinion of some experts a real and not easily solved problem is the authorized user who uses the authority for personal gain or to harm or misuse the computer resources.

3. How Can Definitional Problems be Resolved?

A major barrier to both understanding the subject and developing legislation is the lack of concise universally accepted definitions of the relevant terms and concepts. For example, a persistent problem plaguing the legislators is what constitutes a "computer abuse. A continuing concern is that if a term is defined too broadly it may be subject to misinterpretation while a narrow definition limits understanding of the offense or problem and may hamper prosecution of the computer criminal. Those that have studied the issue claim that a clear definition of "computer abuse" is needed in order to aid in convicting and prosecuting offenders.

Another definitional difficulty is adequately describing some of the other terms associated with "computer abuse". For example, the term "computer" lacks a universally accepted technical definition. Part of the problem is that computer and information technologies are undergoing change. Legislators have found that assigning definitions is a significant challenge. There are also definitional problems with related terms such as "access", "use", "networks", "programs", and "software". The difficulty in constructing concise definitions is reflected in the state computer crime statutes that have struggled with the associated terms (see Chapter III).

4. Is There a Need For Additional Computer Crime Legislation?

Over the years there has been extensive debate on the need for a Federal "Computer Crime" statute. Congressional concern and media attention continue to focus on the problem. In addition, groups, such as the American Bar Association, have called for statutory language to combat computer abuse. The debate centers on two approaches: development of a distinct "computer crime" statute and amending existing laws. Also, certain unique aspects of computer abuse, such as trespassing, browsing, have been identified and may require further assessment.

Concerns have been expressed over innovative applications (e.g., electronic mail) and questions regarding liability and responsibility also have not been fully addressed. The recent enactment of the Federal computer crime law, "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984", contained in P.L. 98-473, is considered by some to be a first step in obtaining a more comprehensive statute. The new law limits the scope of Federal jurisdiction to computers in government, certain banks, and financial institutions, but fails to address problems such as "computer trespassing" and "computer browsing". Supporters of an expanded statute argue that traditional laws addressing physical access do not adequately address the problem of intrusions into a computerized information system.

Additional legal remedies have been proposed that would modify and amend existing statutes. For example, the Communications Act of 1934 does not adequately define the term "interception". Proposals to change the Act to protect against computer abuse are being considered. Another statute, the Crime Control Act, also fails to give a clear definition of "interception". Consequently, it has been suggested that consideration should be given to strengthen such existing statutes to provide an additional level of legal remedies to cope with computer crime.

5. What New Issues Require Further Assessment?

The adequacy of certain traditional methods and processes are challenged by the potential abuse to automated information systems. For example, it is not clear if electronic message/mail systems are protected by the traditional controls of the paper mail systems. It has been suggested that the controls that protect paper mail from unwanted disclosure, interception, and destruction may not be adequate to give protection to electronic mail. Distinct statutory language may be needed to give appropriate protection.

Another example in which traditional protection may be inadequate is in the area of "computer trespassing". Physical trespassing prohibitions are generally understood. Posting a "no

trespassing" sign on property is designed to warn intruders. Often legal remedies can be found for this type of intrusion. It is not clear if a notice on an automated data base gives an equal level of protection. These issues may require special assessment to determine the need for additional legal remedies.

Another issue that may warrant further assessment is the identification and handling of evidential materials in computer crime cases. There has been limited experience in defining what evidential materials are appropriate, and how the material is to be collected and presented. In the opinion of some experts failure to identify and collect evidence in cases of computer abuse is critical.

The legal and technical aspects are difficult to separate in areas such as responsiblility for certification of computer systems and products. The extent of liability if systems do not perform or security products do not provide adequate protection continues to be a much debated subject. An effort should be made to address these issues both from a national perspective as well as from a DoD view.

C. FEDERAL INITIATIVES

1. NSDD-145

The National Security Decision Directive-145 (NSDD-145), "National Policy on Telecommunications and Automated Information Systems Security", issued on September 17, 1984, provides a new policy direction in protecting voice and data communications resources. The new policy is aimed at safeguarding automated information systems with a special focus on protecting those systems accessed via and dependent on network communications. A key objective of the new policy is to develop "a reliable and continuing capability to assess threats and vulnerabilities" and to safeguard information from "hostile exploitation". (Full text of the unclassified version of the NSDD-145 appears in Appendix E.)

The NSDD-145 creates a senior level steering group and an interagency operating level committee, and designates a National Manager to implement the objectives of the new policy. The interagency committee, the National Telecommunications and Information Systems Security Committee (NTISSC), is chaired by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C^3I). The NTISSC is to provide operating policy and guidance. The Director of the National Security Agency (NSA), as National Manager is assigned the

responsibility to assess threats to sensitive systems and to characterize the overall security posture of the agencies.

The newly issued policy requires investments in research and development to provide the appropriate technologies to protect automated information systems. The NSDD-145 provides an opportunity for Federal agencies to improve the ordering of priorities and the allocation of resources to ensure automated information resources against abuses and misuse.

2. U.S. Department of Justice

The Department of Justice (DOJ) has a broad interest in computer abuse and misuses as a result of both statutory and regulatory responsibilities inherent in its mission and programs. The scope of these responsibilities includes enforcement of the law in combatting computer crime, prosecuting and convicting the computer abuser, and training of enforcement officials.

While the various programs and initiatives cannot be totally described here, one initiative has been the Bureau of Justice Statistics sponsored reports and handbooks on computer crime.

> U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime. Criminal Justice Resource Manual. Washington, U.S. Government Printing Office, 1979. 392 p.;

U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime: Electronic Fund Transfer Systems and Crime. Washington, U.S. Government Printing Office, 1982. 182 p.;

U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime: Legislative Resource Manual. Washington, U.S. Government Printig Office, 1980. 66 p.;

U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime: Expert Witness Manual. Washington, U.S. Government Printing Office, 1980. 28 p.; and

U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime: Computer Security Techniques. Washington, U.S. Government Printing Office, 1982. various pagings.

These reports contribute to the understanding of legal and technical aspects of computer-related crimes. This series of reports is designed to provide prosecutors and other criminal justice officials with a framework for understanding some key concepts and problems related to computer assisted crimes. A current effort is underway to augment this series of reports with a review of State and local prosecutors' experience using state computer crime statutes. This study is being conducted by SRI International for DOJ and is scheduled for completion early in 1985.

The Department of Justice studies on computer crime should be viewed as a beginning, as there is every indication that further work is needed.

One specific area which requires support is information and training in the identification and collection of "evidential materials" in cases of computer abuse. Training law enforcement officials on collection of evidence is one means to effectively cope with computer crime. Consequently, consideration should be given to developing additional guidance in identification and collection of evidence.

D. AMERICAN BAR ASSOCIATION (ABA) REPORT[8]

The ABA Computer Crime Task Force conducted an in-depth review of both private and public organizations on the implications of computer crime. The ABA survey pinpointed the type of computer crime, annual losses from computer crime, experiences with computer crime, need for a Federal statute, and future or potential elements that would have implications for computer crime. The ABA Task Force supported the need for computer crime legislation but "reserved comment" on specific language. A summary of the ABA findings appears in Appendix G.

The ABA report examines the results of the survey in context of the major and publicly debated issues. The report refers to[9]:

- The Nature and Importance of Computer Crime

The ABA report calls attention to "unexplained" and "unsupported" estimates of economic losses attributed to computer crime. While the ABA report does not quantify the problem, it does suggest that there is evidence that the problem is of substantial and growing significance.

- Public and Private Sector Response

Responsibility for coping with computer crime must be shared between government and the private sector. Society is subject to two types of costs -- the monetary losses and the resources to be spent on controlling (i.e., preventing, detecting, investigating, prosecuting) computer crime. Primary responsibility for controlling computer crime rests with private industry and the individual users. The ABA report indicates that there is a gap between computer technology and computer security technology and that this gap seems to be increasing.

- The Need for Federal Computer Crime Legislation

The ABA endorsement of a Federal statute on computer crime is supported by the ABA's survey and recent media reports. Legislation, the ABA report concluded, would be beneficial. The ABA reported that a danger exists from the fact that

- that various forms of computer abuse and misuse are illegal and improper and

- a lack of a computer crime statute hampers federal enforcement.

CHAPTER II. FEDERAL LEGISLATIVE ACTIONS

After more than five years of debate, Congress has enacted a "computer crime" law. The new law, "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984", included in the continuing appropriation's P.L. 98-473 is considered a first step to developing appropriate legal remedies. Over the years the Federal legislators have assessed computer abuse by attempting to:

- o understand the scope and nature of computer abuse;
- o identify key issues; and
- o resolve definitional problems.

This chapter reviews some of the relevant congressional actions and legislative initiatives.

A. CONGRESSIONAL INITIATIVES

Congressional examination of computer abuse emerges from a range of legal, economic, and social concerns. Traditionally, the focus has been on safeguarding certain types of information (e.g., personal data, financial information, and criminal justice information), and certain classes of sensitive data which if disclosed could be harmful to the nation (e.g., national security classified information). Congress has enacted a wide range of

legislation to protect certain types of data (e.g., census, and social security data).

Congress continues to focus on improving Federal information technology management and protection of information resources. As discussed above, this has included consideration of statutes to improve government management of information and associated technologies. Since the late 1970s Congress has examined various aspects of computer security. In the mid-1970s attention to protecting computer resources has centered on computer abuses.

1. 94th - 97th Congress

Beginning in the 94th Congress, the then Senate Committee on Government Operations (now the Senate Committee on Governmental Affairs) conducted a series of investigations into computer abuse. Two major congressional reports, issued in 1976 and 1977, by the Senate Committee, (chaired by Senator Abraham Ribicoff), initiated congressional examination of computer fraud and abuse[10].

In the 95th Congress, Senator Ribicoff introduced S.1766, the "Federal Computer Systems Protection Act of 1977". This initial measure received no final action and subsequently, in the 96th Congress, Senator Ribicoff submitted a modified bill, S.240, the "Federal Computer Systems Protection Act of 1979". That

measure, popularly known as the "Ribicoff Bill", addressed four categories of computer crime:

- The introduction of fraudulent records or data into a computer system;

- The unauthorized use of computer-related facilities;

- The alteration or destruction of information or records; and

- The stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data.

Hearings were held in 1978 and 1980 on the "Ribicoff Bill" by the Senate Committee on the Judiciary[11]. The supporters of the legislation contended that the enactment of the legislation not only penalized abusers but would, in their opinion, contribute to improved management of computerized resources. Although the intent of this initial measure was supported, concerns were raised regarding[12]:

o the possible expansion of Federal jurisdiction;

- the lack of accepted and concise definitions;

- danger that new applications, such as electronic message systems, might be hampered in their development;

- the inadequacy of the criminal justice officers to handle technical aspects of a computer crime, such as collecting evidence; and

- the lack of information on the exact scope and dimensions of computer abuse.

In the 97th Congress, Representative Bill Nelson introduced H.R.3970, the Federal Computer Systems Protection Act of 1981. This bill, modeled after the earlier introduced "Ribicoff Bill", received no final action. Nevertheless, hearings were held on the subject of computer crime by the House Judiciary Subcommittee on Civil and Constitutional Rights. At these hearings, witnesses discussed the problems of computer abuse but fell short of supporting specific legislative language. The lack of accurate statistics on computer crime incidences, and the difficulty in understanding the subject continued to be viewed as barriers to developing an appropriate Federal computer crime statutory language[13].

2. Summary of 98th Congress Actions

In the 98th Congress computer abuse was the subject of several hearings[14] and over ten bills were introduced. Details on the legislation appear below.

a. House Committee on the Judiciary

The House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights held specific hearings on computer crime legislation[15]. Witnesses admitted that current Federal statutory language did not contain any specific sanctions dealing with computer crime. John C. Keeney, Deputy Assistant Attorney General of the United States, testified that:

> Any enforcement action in response to criminal conduct indirectly related to computers must rely upon a statutory provision dealing with some other offense. This requires the law enforcement officer, initially the agent, and then prosecutor, to attempt to create a "theory of prosecution" that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even illegal conversion of trade secrets.

Furthermore, Mr. Keeney went on to say that current efforts to prosecute computer criminals can easily be thwarted. He explained that in one instance prosecution was possible under the Federal wire fraud law because the defendant had made two of the fifty access calls across state lines. In another incident, the Langevin case, a former Federal Reserve Board staffer obtained access to a file without authorization. In both instances if the

access had not been interstate the Federal wire fraud statute could not have been applied.

The Committee on the Judiciary Subcommittee on Crime also identified the limitations of Federal statutes to handle computer crime. In the Subcommittee's report (House Report No. 98-894) accompanying H.R5616, "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984"[16], the two cases mentioned above are cited as presenting difficulties in utilizing existing laws to convict the computer criminal. The House panel went on to report that the language contained in H.R.5616 would permit prosecution of these offenders[17]. Subsequently amended, H.R.5616 was enacted in the final days of the 98th Congress. (See discussion of P.L. 98-473 below.)

b. Senate Committee on Governmental Affairs

Early in 1983 the Senate Committee on Government Affairs Permanent Subcommittee on Investigations chaired by Senator William Roth, issued a report on computer security focusing on congressional and executive branch initiatives[18]. The report provides an overview of key issues and discusses relevant Federal agencies activities in support of securing computer-related resources.

In October of 1983 another Subcommittee of the Senate Committee on Governmental Affairs, chaired by Senator William Cohen held hearings on the subject of computer security[19]. These hearings generally focused on the difficulties in understanding the concerns regarding threats to Federal computer-related resources. Senator Cohen subsequently introduced a legislative computer abuse measure S.2270 (discussed below).

c. House Committee on Science and Technology[20]

The House Committee on Science and Technology Subcommittee on Transportation, Aviation, and Materials, chaired by Representative Dan Glickman, held a series of hearings on computer and communications security. While these hearings did not focus on computer crime legislation, nevertheless, testimony given at these hearings concluded that there was a need to strengthen statutory language to cope with computer abuses. The hearings specifically highlighted the problems of electronic "access" and "intrusion" in automated information systems.

An important issue raised at the hearings was whether unauthorized access into a computer system was a Federal crime? In response to this, Floyd Clark, Assistant Director, FBI Criminal Investigations Division, commented:

- Not necessarily: it is possible for an individual to gain access into a computer system, and if there is no damage nor information acquired that in and of itself would not constitute a Federal crime.

Mr. Clark went on to say the computer crime legislation needed better definitions for terms such as "damage", "unauthorized intrusions" and "trespassing". It remains unclear if laws covering physical "trespassing" relate to electronic trespassing or unauthorized accessing of an automated information system. Another problem identified at the hearings related to the term "interception". The General Accounting Office (GAO) commented that the definitions and concepts of such terms required further assessment. Specifically the GAO noted that[21]:

> A review of applicable telecommunication security legislation showed that the Communications Act of 1934 and the Crime Control Act of 1968 are inadequate with respect to interceptions of wire communications, or "wiretapping". The 1934 Communications Act did not define the term "interception". The Crime Control Act of 1968, as amended, used the qualifying term "aural acquisition" (acquired by use of the ear) to define interception. As a result, only interceptions by aural means are illegal under this act, unless authorized by court order. Therefore, we conclude that as long as the term "aural" remains as a semantic qualifier in the 1968 Crime Control Act's definition of interception anyone can conduct unauthorized nonaural wiretapping of data telecommunications without a court order and not be in violation of this law.

A follow up report[22] to the hearings, while not supporting a computer abuse legislative measure, called for the creation of a national commission to examine the issues related to computer

security and to address the implications of computer abuse on society.

B. FEDERAL LEGISLATION (98th CONGRESS)

Over ten bills relating to computer abuse have been introduced in the 98th Congress (1983-1984). (Figure 2 identifies some of these key measures, and full text of selected measures are included in Appendix C.) These bills may be classified into four major categories:

1) Computer crime legislation is generally focused and contains specific penalties for abusing or misusing computerized resources (e.g., H.R.1092, S.2270, S.2940.)

2) Computer crime legislation associated with other requirements or other distinct tasks. (e.g., H.R.5616 Counterfeit Access Device and the Computer Fraud and Abuse Act of 1984 in P.L. 98-473)

3) Computer abuse legislation which focuses on instituting preventive measures to limit unwanted computer abuse activities. (H.R.3075/S.1920 now P.L.98-362, the Small Business Computer Security and Education Act of 1984)

4) Computer crime legislation which provides for the protection of one set of records (e.g., medical records) (H.R.5954).

Many of the Federal computer crime bills, while similar in intent, contain variations in scope and minor language differences directed at limiting the prohibitive behavior. This section discusses the new Federal computer crime law and a few of the computer crime bills introduced in the 98th Congress, including the Administration Bill S.2940, and the Small Business Computer Security and Education Act of 1984 (P.L. 98-362). The status of the legislation is summarized in Figure 2 below.

Figure 2

SELECTED COMPUTER RELATED ABUSE MEASURES CONSIDERED IN THE 98TH CONGRESS

Bill No. Sponsor	Title	Action/Status
P.L.98-473 (Formerly H.R.5616 (Rep. Hughes))	Counterfeit Access and Computer Fraud and Abuse Act of 1984.	Included in continuing appropriation bill as part of the crime prevention provisions.
H.R. 1092 (Rep. Nelson)/ S.1733 (Sen. Trible)	Federal Computer Systems Protection Act of 1983	House bill subject of hearing by House Committee on the Judiciary. No action on Senate bill.
P.L.98-362 (Formerly H.R. 3075 (Rep. Wyden)/ S.1920 (Sen. Tsongas))	Small Business Computer Security and Education Act of 1984	Being implemented by Small Business Administration.
H.R.4301 (Rep. Coughlin)	Provides penalties for Computer Abuses.	Bill subject of hearings Computer Abuse Committee on the Judiciary.
H.R. 4384 (Rep. Mica)	Establishes computer security Research program, intragency group, penalties misuse and abuse of computerized resources	Bill subject of hearings by the Committee on the Judiciary.
H.R. 4954 (Rep. Wyden)	Medical Records Protection Act of 1984	Hearings by House Committees on Energy and Commerce and the Judiciary.
S.2270 (Rep. Cohen)	Computer Crime Prevention Act of 1984	Referred to the Senate Committee on the Judiciary.
S.2940 (Sen. Thurmond)*	Federal Computer Systems Protection Act of 1984	Referred to the Senate Committee on the Judiciary.

* Referred to as the "Administration Bill"

1. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, P.L. 98-473

The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 was enacted as part of the crime prevention provisions included in the continuing appropriations (P.L. 98-473). The new law, derived from H.R. 5616, amends Chapter 47 of Title 18 and provides penalties for fraud and related activities in connection with access devices and computers. The version agreed to by the Congress narrows the scope of the Act to Federal computers and certain banks and financial institutions. The Act specifically focuses on fraud in connection with computers.

The Act primarily prohibits the unintended use, modification, destruction, or disclosure of information in government computers. The new law specifically protects against unauthorized disclosure of information related to national defense, foreign relations, or other restricted data. The law is invoked if the "intent" or "reason" behind such disclosure is to injure the United States or is advantageous to a foreign nation.

For a first offense penalties under this bill consist of a fine of not more than $10,000 or twice the value obtained and/or ten years imprisonment; for a second offense punishment will consist of a fine $100,000 or twice the value obtained and/or twenty years imprisonment.

The law defines the term computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device but such a term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device".

2. Federal Computer Systems Protection Act of 1983 (H.R.1092)

H.R.1092, introduced by Representative Bill Nelson, and S.1733, introduced by Senator Paul Trible, are identical bills directed at penalizing the fraudulent or illegal use of computers. These measures evolve from the earlier "Ribicoff" bills and affect Federal government and financial institutions, computers, and those computers that "operate in, or use a facility of interstate commerce". Consequently the bill, if enacted, would effect a larger number of computers than the new Federal computer crime statute (P.L. 98-473). This feature of the bill is perceived as broadening Federal jurisdiction; it contrasts sharply with the new law and S.2940, the "Administrations Bill" (described below).

H.R. 1092 does not specify any dollar amount of damages before the law is invoked but rather it is based on intent. The bill H.R. 1092 provides that it is a crime if:

> The intent (is) to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations or promises, or to embezzle, steal or knowingly convert to his use or the use of another.

The bill provides for the following penalties to be levied against the computer criminal; "a fine of three times the gain or $50,000, which ever is higher". In addition to a fine, the computer criminal may receive a prison term of up to 5 years, or both. Intentional damage or destruction to the systems and resources covered by the legislation would result in similar penalties.

The measure includes a set of definitions for some of the technically related terms, such as "computer", "property", "services", "use", and "computer medium". As defined in H.R. 1092, the term "use" seemingly expands the intent aspect by including:

> access, instruct, communicate with, store data in or retrieve from, or otherwise utilize logical or arithmetic or memory function of a computer, or with fraudulent or malicious intent, to cause another to put false information into a computer.

H.R.1092 has been the subject of hearings by the House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights but has not received final action.

3. Federal Computer Systems Protection Act of 1984 (S.2940)

On behalf of the Administration, Senator Strom Thurmond introduced S.2940, on August 9, 1984. This bill, like the others reviewed above, amends Chapter 47 Title 18, U.S. Code by adding a new section. The Administration Bill attempts to narrow the focus by including only three categories of computers to be affected by the measure. Specifically, it distinguishes computers owned or operated by, under contract or operated in behalf of:

- the United States Government; or
- a financial institution; or
- two or more computers located in different states or in a State and a foreign country.

The bill makes it a Federal felony offense to engage in computer-related fraud or theft, damage, or destruction of associated resources (e.g., data, computer program). Under this bill an offender could be fined twice the amount of gain or $50,000 (which ever is higher) or imprisoned up to five years.

The bill advances the concept of "unauthorized access" and makes it a misdemeanor to "intentionally and without authorization access a computer, computer system or network owned or operated by the Federal government or a federally insured financial institution". Offenders of this unauthorized access provision could be fined up to $25,000 or receive a prison sentence of not more than one year, or both.

An important departure in the Administration Bill is that it permits confiscation of computer and related devices which are used to commit the prohibited action. The bill defines key terms related to computers (e.g., "computer", "computer systems", "computer programs", "computer software", "computer services") but defines "access" as including actions which:

> instruct, communicate with store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or computer network.

4. Computer Crime Prevention Act of 1984 (S.2270)

S.2270 introduced by Senator William Cohen, similar to H.R.1092 and S.1733, contains additional clarifying language on the object of the bill. Specifically, it provides penalties for one who "knowingly, intentionally, and without authorization,

directly or indirectly uses or attempts to use any computer to defraud, obtain money, or property... by means of false or fraudulent pretenses, representation, or promises".

The measure, S.2270, directly involves or affects computer operations for or in behalf of the Federal government or financial institutions. In addition, H.R.1092 affects all computers "operating in or using a facility of interstate commerce". The measure introduced by Senator Cohen has been referred to the Senate Committee on the Judiciary and has not received additional action.

5. Other Computer Crime Relate Measures

Using contrasting approaches, both H.R.4384, introduced by Representative Dan Mica, and H.R.4301, sponsored by Representative Coughlin attempt to cope with computer related crimes. H.R.4384 is a complex omnibus measure, while H.R.4301 is highly focused.

For example, H.R.4384 would establish penalties for computer crimes, support a computer security research program (administered by the U.S. Department of Commerce), and create an interagency committee on computer crime and abuse. As proposed in the measure, this interagency committee would be responsible for:

- o establishing a clearinghouse for information related to fraud and abuse;

- o coordinating computer security research;

- o making recommendations to improve the security of Federal computer system; and

- o reporting to the Congress regarding statutory changes to protect computers from fraud and abuse.

In H.R.4384 the computer fraud and abuse section is identical to H.R.1092.

The Coughlin measure, H.R.4301, addresses only computer-related crime. The bill refers to computers affecting both interstate and foreign commerce. The bill specifically sets the penalty for specific abuse and unauthorized use at $100,000 or imprisonment of ten years, or both.

6. Small Business Computer Security and Education Act of 1984, P.L. 98-362

The increased dependence of small business increase dependence on computers and associated technologies prompted Congress to enact a law to assist in protecting these resources. While the Small Business Computer Security and Education Act of

1984 is not a criminal statute, it highlights some important issues. P.L. 98-362 is designed to foster an understanding of computer abuse and promote effective computer security management. The Act creates the Computer Security and Education Advisory Council composed of officials from the Federal government[23] and the private sector. This council is to advise the Small Business Administration on:

- the nature and scope of computer crimes committed against small business concerns,
- the effectiveness of Federal and state law in deterring computer-related criminal activity or prosecuting computer related crimes,
- the effectiveness of computer technology and management techniques available to small business for increasing computer security,
- the development of information and guidelines to be made available to the (SBA) Administrator to assist small business concerns in evaluating the security of computer systems.

The Act establishes a computer security and education program to assist small business concerns with a better

understanding of the use and management of computer technology. It directs that (1) a computer crime forum be developed and (2) training support to educate small business concerns be developed.

C. COMPARISION OF SELECTED ELEMENTS OF PENDING BILLS

1. Definitions

The current Federal bills on computer abuse provide definitions on key terms which have distinct technical aspects. For example, most of the Federal legislative measures attempt to define the term "computer" - this has not been easy. Like so many of the state statutes the Federal measures have had some difficulty in fully capturing the essence of the technical terms. Consequently the term "computer", as employed in the Federal measures, is often described as:

> an electronic, magnetic, optical hydraulic, organic or other high speed data processing device or system performing logical, arithmetic or storage functions, and includes any property, data storage facility or communications facility directly related to or operating in conjunction with such device or system.

In H.R.1092/S.1733 and S.2270 the definition of a "computer" excludes an "automated typewriter or typesetter, a portable hand-held calculator or any computer designed manufactured and used

exclusively for routine personal, family, or household purposes and which is not used to access, communicate with, or to manipulate with any computer".

Computer crime is a concept addressed by the pending bills but not always defined. The Small Business Computer Security and Education Act of 1984 (P.L. 98-362) does give a limited description of the concept as:

- o any crime committed against a small business concern by means of the use of a computer, and
- o any crime involving illegal use of or tampering with a computer owned or operated by a small business concern.

Another concept that has been difficult to define is "trespassing" or "browsing" in a computer system. The Administration Bill, S.2940, does attempt to address "computer trespassing" by relating to "intentional and unauthorized" access.

2. Penalties

In the Federal measures considered by the 98th Congress there is very little variation regarding penalties. This is reflected in the fact that the language of S.2940, H.R.1092, and S.2270 provide that the fine be not more than twice the amount or

$50,000, which ever is higher, and imprisonment is for five years.

The new Federal computer crime statute (P.L. 98-473) provides penalties for first offenses of a fine of $50,000 or twice the value, whichever is greater, with a possible sentence of ten years. Those with previous convictions would be fined $100,000 or twice the value whichever is greater, and may be given a possible sentence of twenty years.

In addition, S.2940, the Administration Bill, creates a penalty for intentional unauthorized access as a misdemeanor in which the fine may be $25,000 or a year in prison or both. As mentioned above, S.2940 permits confiscation of computers and associate equipment used in the prohibited activity. Specifically, the bill provides that:

> Upon conviction...the court shall authorize the Attorney General to seize all property or other interest...

The provision to confiscate computer devices is unique to S.2940 and is believed to provide an important deterrent.

CHAPTER III. STATE COMPUTER ABUSE STATUTES

Approximately thirty-four states currently have laws which may be broadly classified as "a computer crime statute". A number of states have bills pending and, in one instance, the New York State legislature passed a bill, although it was recalled for further consideration.

Selected states identified as having computer abuse statute (see Appendix D for complete citations) include:

1.	Alaska	18.	Missouri
2.	Arizona	19.	Montana
3.	California	20.	Nevada
4.	Colorado	21.	New Mexico
5.	Connecticut	22.	North Carolina
6.	Delaware	23.	North Dakota
7.	Florida	24.	Ohio
8.	Georgia	25.	Oklahoma
9.	Hawaii	26.	Pennsylvania
10.	Idaho	27.	Rhode Island
11.	Illinois	28.	South Dakota
12.	Iowa	29.	Tennessee
13.	Kentucky	30.	Utah
14.	Maryland	31.	Virginia
15.	Massachusetts	32.	Washington
16.	Michigan	33.	Wisconsin
17.	Minnesota	34.	Wyoming

The State laws range from complex with encompassing definitions to those which are quite narrow and focused. Many of the state statutes are modeled after the "Ribicoff Bill" (S. 240).

As has been discussed, states have depended on the traditional crime statutes, for fraud or corruption, e.g., to combat computer crimes. Concern for protecting information resources at the State level also is not new concept. Traditionally State governments have been supportive of information protection. This is reflected in the fact that more than half of the states have specific laws protecting certain types of data (e.g., personal data, medical, financial, tax, criminal justice and educational records, as well as trade secrets). These laws provide a foundation for information protection and in a few instances have been viewed as including misuse or abuse of associated computer-related resources. Advocates of specific computer crime legislation have argued that these laws alone are not sufficient to address computer-related crime.

A. ANALYSIS OF SELECTED STATE LAWS

1. Computer Crime - The Concept

Variations in state statutory language reflect an attempt to come to grips with conceptual and definitional problems. Consequently the state computer crime statutes reflect not only the evolution of the state code of laws but the influence of the Federal bills (e.g., the Ribicoff Bill) as well as other state bills.

The lack of a universally accepted set of definitions relating to computer abuse has been met by states by developing a range of alternative definitions for "computer crime", "computer theft", "computer fraud", and "computer misuse", etc.. For example, Delaware's computer crime statute outlines both computer fraud and computer misuse and distinguishes those committing computer fraud as:

> whoever knowingly and willfully, directly, without proper authorization, accesses or attempts to access any computer, computer system, computer network or any part of same for the purpose of:
>
> (1) devising or executing any scheme to defraud the owner thereof or any company, government client or person who may be so defrauded, or
>
> (2) obtaining money, property, or services for themselves or another by means of false or fraudulent pretense, representations, or practices shall be guilty of computer fraud.

and computer misuse as:

> whoever intentionally and without proper authorization directly or indirectly accesses, alters, damages, modifies, destroys or attempts to damage or destroy any computer for an improper purpose shall be guilty of computer misuse.

The Arizona law expands this classification slightly by relating to the symbolic use of a computer. The statute states that a crime is committed by:

> accessing, altering, damaging or destroying without authorization any computer, system or network, with the intent to

devise or execute any scheme or artifice to defraud or deceive or control - property or services by means of false or fraudulent pretenses or representations.

Another perspective is brought to the subject by other state statutes which address "unlawful use". The Illinois state statute, for example, provides that a person commits unlawful use of a computer when he:

(1) Knowingly obtains the use of a computer system, or any part thereof, without the consent of the owner or

(2) Knowingly alters or destroys a computer system or any part thereof, without the consent of the owner or

(3) Knowingly obtains the use of a computer system, or any part thereof, as part of a deception for the purpose of obtaining money, property or services from the owner of the computer system or any third party.

This concept is delineated further in the Colorado state statute which states that:

(1) Any person who knowingly uses any computer system, computer network or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization or committing theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network... or any computer program, documentation, or data contained in such computer, computer system or computer network commits computer crime.

2. Definitions

State computer crime statutes often include definitions of key terms designed to clarify the scope and intent of the measure. These definitions are designed to provide the necessary clarifying language to aid in enforcement of the law. As previously mentioned the definitions in State computer crime laws are not always uniform and often reflect the pre-existing statutory framework or legal evolution within the specific jurisdiction. Figure 3 indicates terms identified in some of the States computer crime laws.

The terms frequently defined in the State statutes include "computer", "access", "network", "program", "software system", "property" and "services". Less frequently defined were the following terms: "data", "authorization", "use", and "intellectual property". A few States, such as Alaska, did not provide any definitions. The more important terms are treated in some detail below.

Figure 3

Computer-Related Terms Defined in selected State Statutes

	STATE	Access	Computer	C.Network	C.Program	C.Software	C.System	Data	Financial Instrument	Property	Services	Authorization	Use	Intellectual Property
1.	Alaska													
2.	Arizona	X	X	X	X	X	X		X	X				
3.	California	X		X	X		X	X	X	X	X			
4.	Colorado *	X	X	X	X	X	X		X	X	X	X	X	
5.	Connecticut ooo	X	X	X	X	X	X	X		X	X **			
6.	Delaware	X	X	X		X	X	X		X		X		
7.	Florida	X	X	X	X	X	X			X	X oo			X
8.	Georgia	X	X	X	X	X	X	X	X	X	X			
9.	Hawaii	X	X	X	X	X	X	X	X	X	X			
10.	Idaho	X	X	X	X	X				X	X			
11.	Illinois		X		X		X							
12.	Iowa o	X	X	X	X	X	X	X		X	X			
13.	Maryland ooo	X	X	X	X	X	X				X			
14.	Michigan									X	X			
15.	Minnesota	X	X	X	X	X	X			X	X			
16.	Missouri	X	X	X	X	X	X		X	X	X			X
17.	Montana													
18.	New Mexico	X	X	X	X	X	X						X	
19.	Nevada		X	X	X		X	X		X				
20.	North Carolina	X	X	X	X	X	X		X	X	X			
21.	North Dakota													
22.	Ohio		X	X	X		X	X						
23.	Oklahoma *	X	X	X	X	X	X			X	X			
24.	Pennsylvania													
25.	Rhode Island	X	X	X	X	X	X			X	X			
26.	South Dakota		X		X		X							
27	Tennessee oo	X	X	X	X	X	X	X	X	X	X			X
28	Virginia		X	X	X	X		X	X		X			
29	Utah oo oo	X	X	X			X		X		X			
30	Wisconsin		X	X	X	X	X	X	X	X				

* Defines "supporting documentation".
** Includes Computer service system.

o Defines "loss of property" and "loss of services".
oo Defines "process".
ooo Defines "private personal data".
oooo Defines "software/program" as one.

a. Computer

Perhaps one of the more controversal definitions given in state computer crime statutes is the term "computer". Since "computers" are associated with an evolving set of technologies the term lacks a universally accepted definition. Consequently, states have had to grapple with the problem of developing the term. For example, the Arizona State Statute defines the computer as:

> an electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication, facilities which are related to such a device in a system or network.

This definition can be compared to the more cryptic definition in the Florida Statute in which "computer" is simply defined as "an internally programmed, automatic device that performs data processing". The Florida definition has been criticized because it is imprecise and may be interpreted to include many more devices then had been envisioned by the drafters of legislation; It has been suggested that the term "device", as described in the Florida statute, may be interpreted perhaps to include a large scale computer system, a desktop calculator, an electronic wrist watch, the telephone, and electronic fare cards such as are used on the Metro or city transportation systems.

A more comprehensive definition of "computer" is illustrated by the computer crime bill passed but recently recalled by the New York State legislature. The recalled measure attempted to clarify the nature of "computer" by giving it the following meaning:

> a device or group of devices which, by manipulation of electronic or magnetic impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device equipment or facility which enables the computer to store, retrieve or communicate to or from a person, another computer or other device the results of computer operations, computer programs or computer data.

b. Access and Use

The term "access", defined in more than half the state statutes, is described as a technical approach for obtaining information/services via computerized resources. For example, Florida and Arizona, as well as other states, describe "access" as "to approach, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network."

The California statute attempts to provide additional clarity regarding the term "access". In that law it is defined as an "approach, a way or means of approaching, nearing, admittance to, including to instruct, communicate with, store

information in or retrieve information from a computer system or computer network".

Some state computer crime statutes emphasize the close relationship between "access" and "use". In one instance, (e.g., Montana state statute) defines "access" as:

> to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from or otherwise make use of any resources of a computer, computer system, or computer network or to cause another to instruct, communicate with, store data in, retrieve data from, cause input to, input from, or otherwise make use of any resources of a computer, computer system, or computer network.

c. Data and Intellectual Property

Approximately one third of the states define "data" but just a few States equate it with the phrase "intellectual property". Wisconsin State statute describes "data" as "a representation of information, knowledge, facts, concepts or instructions that have been prepared or is being prepared in a formalized manner and has been processed, is being processed or is intended to be processed in a computer system or computer network." The Wisconsin law goes on to state that "data may be in any form including printouts, magnetic storage, disc, punch cards and as stored in the memory of the computer". It concludes that "data are property". A similar concept is articulated in the California law, as well as a few other state statutes.

The Georgia state statute attempts to provide a link between "data" and "intellectual property" by equating the terms. The Georgia statute elaborates on the term "data" by delineating the "form" that the data may take and equating this form to include, but not be limited to, "computer printouts, magnetic storage media, punchcards, or stored internally in the memory of the computer".

d. Other Related Technical Terms

Consideration of computer crime legislation has required defining terms which may not always be adequately described in the technical literature. Consequently, in drafting state legislation there has been a struggle to derive definitions acceptable and understandable from a legal as well as a technical perspective. In some instances the definitions are derived from the technical experience but modified in some instances to meet state statutory framework. Most commonly defined terms include: "software", "program", "computer program", "computer system", "computer network", "computer services", "property", and "financial instrument". Examples of the definitions are included in Figure 4 below.

Figure 4

FREQUENTLY DEFINED TERMS IN SELECTED STATE STATUTES

Term	Definition
Software or Program	A series of instructions or statements in a form acceptable to a computer, relating to the operations of the computer, or permitting the functioning of a computer system in a manner designed to provide results therefore, including programs, application programs, or any copies thereof. (Utah)
Computer Program	A series of instruction or statements, in a form acceptable to a computer, which permits the functioning of computer system in a manner designed to provide appropriate products from such computer system. (Arizona)
	An ordered set of instructions or statements, and related data that when automatically executed in actual or modified form in a computer system, causes it to perform specified functions. (California)
Computer Software	A set of computer programs, procedures and associated documentation concerned with the operation of a computer system. (Arizona)
Computer System	A machine or collection of machines, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control. (California)

(Figure 4 Cont.)

Term	Definition
Computer Network	An interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnecting computers. (Arizona)
Computer Services	Includes, but is not limited to, the use of computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network. (California)
Property	A financal instrument, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible. (Arizona)
	Includes, but is not limited to, financial instruments, data, computer programs, documentation associated with data and computer systems and programs. (Georgia)
Financial Instrument	Any check draft, money order certificate of deposit, letter of credit, bill of exchange, credit card, marketable security or any other written instrument.

B. INITIAL EXPERIENCE

A cursory review of states using their computer crime statutes indicates that only a few States have had experience in prosecuting or convicting violators of the laws. In part this many be attributed to the newness of these laws. As previously mentioned, the lack of information on experiences with computer crime legislation prompted DOJ Bureau of Justice Statistics to sponsor a comprehensive survey of state prosecutors. This nationwide survey being conducted by SRI International is designed to provide information on current experiences and insight into how computer crime laws are being used.

The Florida experience with using the state computer crime statute was detailed in hearings before the House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights. In testimony before the Subcommittee, Assistant State Attorney General James F. Falco outlined his experience with the Florida computer crime legislation by describing the case of the State of Florida v. Diane Smith Torres, Mr. Falco claimed that although hampered by a lack of good communication among various state officials, the case provided an opportunity to put the Florida computer crime statute to use. The defendant Diane Torres was initially arrested on a single count of grand theft and she confessed. A distinguishing factor of the case is that the victim of the crime, Connecticut General Insurance Corporation,

was located in Connecticut but the terminal used in the theft was in Miami.

In Mr. Falco's opinion, the case raised some serious statutory definitional problems. Consequently, Mr. Falco thought that attention should be given to developing strong definitions to avoid ambiguity and to limit possible confusion.

Mr. Falco elaborated that from his perspective there was a distinct advantage to having a computer crime statute. He specifically indicated that the value of "a modern piece of computer crime legislation" is the ease with which evidence can be prepared and admitted, especially when the inevitable computer expert witnesses, private and governmental alike, testify. Mr. Falco went on to comment that:

> the necessity for modern computer crime legislation at the sentencing stage of a prosecution was made perfectly clear in the Torres sentencing.... Diane Torres received seven years on the computer crime count and two concurrent five year terms on the insurance fraud and grand theft counts.

The limited opportunities in states to prosecute the computer criminal is not only as a result of the newness of the legislation but also may be due to the limited understanding by the law enforcement and other criminal justice officials.

Experiences of the states and Federal prosecutors should be evaluated to determine the difficulties and problems. Within the

DoD, information on the experience of enforcement and prosecutorial direction should be fully assessed.

CHAPTER IV. DIRECTIONS AND OPTIONS

Current and future computer requirements prompt consideration of innovations to limit computer abuse. This chapter summarizes the technical implications of abuse, the specific problems confronting the DoD, and some of the approaches that may aid in identifying factors limiting computer abuse.

DoD dependence on computer-related technologies and associated resources is on the increase. This is reflected in the fact that:

- DoD long-range plans indicate that 75% of technology has an important and essential computer component[24];
- More valuable and sensitive data (e.g., financial, inventory, personnel, manpower requirements, and logistics) are being processed on network dependent automated information systems;
- More network and communications systems are being developed; and
- "User friendly" systems are being developed which foster greater use of computer resources.

A. IMPLICATIONS FOR DEFENSE

As has been mentioned, DoD has a long tradition of protecting certain classes of data, in particular, national security classified information. Recently other classes of data not necessarily classified, have been identified as sensitive to the management and operation of the Department of Defense. Consequently, not only national security classified data requires protection but other sensitive data must be identified and safeguarded as well. Although the extent of threats to these data is not always known, there is recognition that unwanted disclosure, manipulation, or destruction of sensitive information represents a serious problem to the DoD and other governmental organizations. The recently issued NSDD-145, if properly implemented, may be a means toward addressing some of these problems.

Before safeguards can be applied the threats and range of abuses must be appreciated. Further assessment of abuse to certain applications may be needed. Abuses in financial systems are perhaps most widely understood but the danger to other systems has remained obscured. For example, there have been allegations regarding tampering with fire control data which reportedly misreacted and failed to respond to specific geographic coordinates. In the past, this class of abuses has

received little if any consideration. Technological initiatives being undertaken by the Department of Defense in which computers are critical deserve evaluation as to the potential for abuse. For example, DoD has embarked on a series of technological innovations in which the security aspects are not always fully known such as artificial intelligence (AI), supercomputers, and development of high order languages.

Within DoD the scope of computer abuse is not known. Although it is beyond the scope of this paper to assess incidents of DoD computer abuse and misuse, the problem certainly deserves additional attention. The real and potential threat to sensitive DoD computerized resources must be assessed in light of the importance of these innovations to the DoD management and operations.

Another set of factors influencing computer abuse is the growing trend towards declassification of certain information. This policy, which is designed to permit the flow of information formerly protected by National Security classification constraints to be more widely available, should be examined closely. Technical data exchange policies contribute to increased dissemination of "sensitive" information. These policies may contribute to increasing the availability of sensitive data; they cannot be entirely ignored if sensitive automated data is to be protected. There may be a need to assess

a wider range of DoD policies to identify actual and potential dangers related to automation of information resources.

This arena may require further study to fully understand the:

1) range of threats from computer abuse and misuse,
2) dangers from related National and DoD Policies, and
3) assessment of tools and techniques to thwart abuses.

B. NEW APPROACHES AND CHALLENGES

Given the importance of computers to conducting the business of the Department of Defense consideration must be given to strengthening current approaches and considering stronger statutory language to combat computer abuse and to limit misuse of these assets. Attention should be given to:

- encourage the development and use of computer security technologies by providing incentives to both manufacturers and users;

- promote analyses and assessments of computer abuse in order to develop a range of appropriate safeguards to be applied to safeguard computerized resources;

- ensure that investigators, prosecutors, and auditors in the enforcement and criminal justice communities have the training to detect, collect evidence, and convict the computer criminal;

- improve coordination of computer security research especially between government and the private sector;

- improve reliability of computer security measures by establishing a certification program;

- increase awareness of the problems by educating users, managers, and others; and

- develop a realistic method to assess threats and vulnerabilities as well as protective measures including documentation and development of standards.

In addition, consideration should be given to developing appropriate statutory language to:

- strengthen existing laws so they may be better used to combat computer abuse;

- enhance definitions and concepts ("computer abuse", "computers", "access", "data", etc.), to improve application of the law;

- create a focus to coordinate and improve training for the enforcement officials;

- create a clearinghouse to promote appropriate sharing of information on security methods and techniques; and

- codify certain objectives of the NSDD-145 to provide a long-term and consistent approach to coping with computer abuse.

C. CONCLUSIONS AND RECOMMENDATIONS

The public debate on computer abuse reflects a diversity of opinion within the technical and legal communities on how to effectively protect against abuse of computer-related resources. The constructs of the existing legal framework focuses attention on the drafting of additional statutory computer crime laws. Because of the novelty of the concept of "computer crime" and the limited experience with both Federal and state computer abuse statutes, there is not available sufficient practical knowledge. Nevertheless computer abuse seems to pose a significant problem

to a nation dependent on automated information processes. Consequently it may be appropriate at this juncture to consider:

- o A legal assessment of existing Federal statutes to pinpoint strengths and weaknesses of current laws in combatting computer-related crime.

- o Identification of legal and technical aspects that improve and facilitate computer abuse reporting.

- o Assess the DoD experiences to date with combatting computer abuse.

- o An "early warning" system to identify potential abuses related to new information technologies.

- o All new DoD computer systems containing sensitive, but not necessarily national security classified data, should be assessed to determine threats and the danger of abuse.

Currently data processing technology is advancing rapidly but computer security technology is not keeping pace. The result is a technology gap that limits implementations of appropriate safeguards. It is therefore important to:

- identify specific computer security features that can be designed as integral elements within the computer hardware and software, especially advanced innovations such as artifical intelligence, expert and knowledge base systems, supercomputers, and the high order languages;

- support and implement reliable security features that not only limit abuses but do not burden systems performance or add excessively to the costs;

- promote computer security administrative measures, especially those that enhance performance and increase reliabilities; and

- improve security technology insertion efforts by institution incentives and an "early-on" identification of appropriate innovations along with a directed program for implementation.

Current Federal efforts to assimilate computer crime statistics are limited. In addition, more information on the experience to prosecute and convict computer criminals is needed. Given the new policy focus of the NSDD-145 it is recommended at this time that there should be a concentrated effort to:

- encourage and reward effective implementation of measures to monitor and control computer abuses;

- promote computer security standards in sensitive systems; and

- encourage development of technologies that identify in real time intrusions into the automated information systems.

Computers and associate technologies have a vital role within the DoD. Protecting these resources from abuse and misuse gives attention to developing an appropriate legal framework. The sensitivity and value of DoD systems suggests there is a real and potential threat to computer related resources. While it is not clear to what extent DoD computer-related resources are subjected to abuse and misuse, it must be assumed that those systems that are not protected are potentially vulnerable to such threats.

Consequently it is recommended that the DoD should:

- improve identification of potential opportunities for abuses and misuses of DoD computer related resources

and assess possible difficulties in prosecuting offenders;

- o implement a department-wide computer abuse prevention program to aid in the monitoring and controlling of unwanted actions, and develop specific administrative and technical measures to reduce computer abuse;

- o improve training of DoD enforcement officials and security officers in identifying and collecting evidence on computer abuse;

- o raise awareness of the dangers of computer abuse with emphasis on penalties for those responsible for abuses;

- o expand research and development on preventive measures and provide standards on procedures and software;

- o embark on an effort to raise awareness of computer security problems by education of high level managers;

- o assess the legal value of the equivalent of a "no trespassing" notice on a system and special notification to users; and

- develop risk assessment models for prototype processes to improve implementation of appropriate safeguards.

FOOTNOTES

1 American Bar Association Criminal Justice Section Task Force on Computer Crime. Report on Computer Crime. Washington, 1984, p.37. (Hereafter referred to as ABA Report.)

2 U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime. Criminal Justice Resource Manual. Washington, U.S. Government Printing Office, 1979, p.3.

3 U.S. Congress. House. Committee on Science and Technology. Subcommittee on Transportation, Aviation and Materials. Computer and Commuications Security and Privacy. Hearings 98th Congress 1st Session held Sep. 26, Oct. 17, 24, 1983. Washington, U.S. Government Printing Office., 1983, p. 72. (Hereafter referred to as U.S. Congress House Committee on Science and Technology Hearing.) (On Sep. 24, 84 the Subcommittee held another hearing on this subject but the hearings document has not been issued.)

4 ABA Report. op.cit., p.43.

5 U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Justice Computer Systems Protection Act of 1979. Hearings on S.240 held Feb. 28, 1980, 96th Congress. 2d session, Washington, U.S. Government Printing Office, 1980. p.1-2.

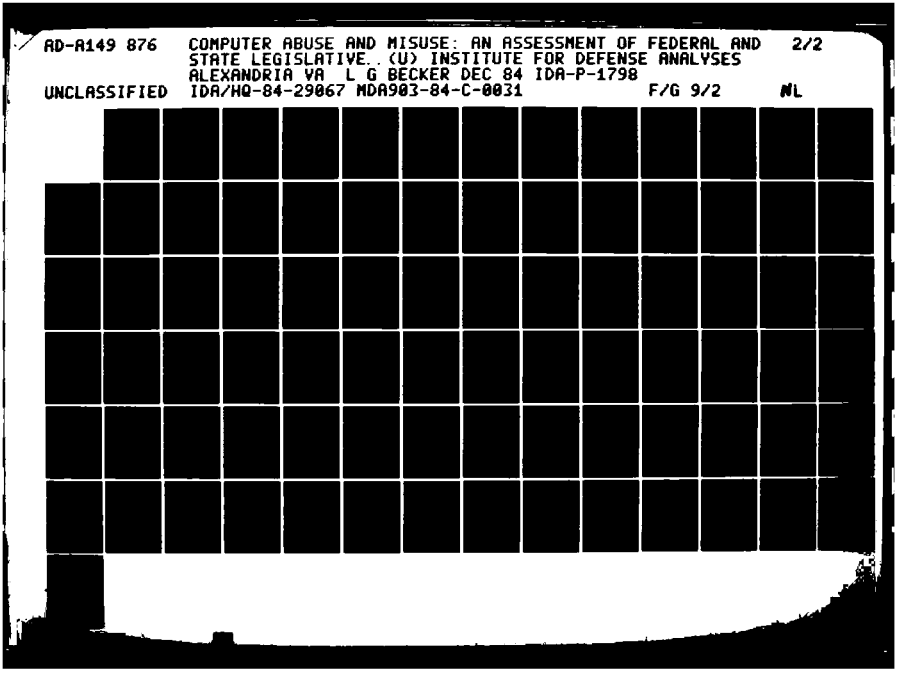
6 U.S. Congress. House. Committee on Science and Technology., op.cit., p.414.

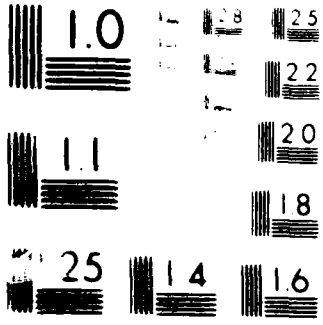
7 U.S. Congress Senate Committee on Governmental Affairs. Subcommittee on Oversight of Government management. Computer security in the Federal Government and the private sector. S. Hearing 98-440. 98th Congress 1st Session. Washington, U.S. Government Printing Office, 1983. p.34.

8 ABA Report, op.cit.

AD-A149 876 COMPUTER ABUSE AND MISUSE: AN ASSESSMENT OF FEDERAL AND STATE LEGISLATIVE.. (U) INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA L G BECKER DEC 84 IDA-P-1798 2/2

UNCLASSIFIED IDA/HQ-84-29067 MDA903-84-C-0031 F/G 9/2 NL




1.0
1.1
25
1.4
1.6
2.5
2.2
2.0
1.8

9 Ibid.

10 These two landmark studies include:

(1) U.S. Congress Senate. Committee on Government Operations. Problems Associated with Computer Technology in Federal Programs and private Industry: Computer Abuse. Committee print, 94th Congress 2d session, Washington, D.C. U.S. Government Printing Office, 1976. p.448 and

(2) U.S. Congress Senate, committee on Government Operations. Computer Security in Federal Programs. Committee Print, 95th Congress 1st session, Washington, D.C., U.S. Government Printing Office, 1977. p.267.

11 U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Federal computer Systems Protection Act. Hearings on S1766, held June 21 and 22, 1978, 95th Congress 2nd session. Washington, U.S. Government Printing Office, 1979.

12 U.S. Congress Senate Committee on the Judiciary. Subcommittee on Criminal Justice. Computer Systems Protection Act of 1979. Hearings on S.240, held February 18, 1980, 96th Congress. 2d Session, Washington, U.S. Government Printing Office, 1980, p.179.

13 U.S. Congress. House. Committee on the Judiciary. Subcommittee on Civil and Constitutional Rights. Federal Computer Systems Protection Action Hearing held Sep 23, 1982. 97th Congress 2d Session. Washington, U.S. Government Printing Office, 1982.

14 The House Committee on the Judiciary Subcommittee on Crime chaired by Representative William Hughes held hearings on accessing protection of credit card. The House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights, chaired by Representative Don Edwards, held hearings on several of the "computer crime" bills including H.R.1092 (Nelson), H.R.4384 (Mica), H.R.4301 (Coughlin).

15 U.S. Congress House Committee on the Judiciary Subcommittee on Civil and Constitutional Rights. Computer Crime hearings on HR 1092, etc. Nov 18, 1983. (unpublished)?

16 U.S. Congress House Committee on the Judiciary. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, House Report No. 98-894, July 24, 1984 (To accompany HR 5616), Washington U.S.Government Printing Office, 1984. Hereafter referred to as House Report No. 98-894.

17 Ibid., p.7.

18 U.S. Congress. Senate. Committee on Governmental Affairs. Permanent Subcommittee on Investigations Federal Computer Security: An Analysis of Congressional Initiatives and Executive Branch Responsibilities. Report prepared by the Congressional Research Service Library of Congress. 98th Congress 1st Session. Washington, U.S. Government Printing Office, 1983, p.45.

19 U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on Oversight of Government Management. Computer Security in the Federal government and the Private Sector. 98th Congress 1st Session. S. Hrg, 98-440. Washington, U.S. Government Printing Office, 1983, p.504.

20 U.S. Congress. House. Committee on Science and Technology, op.cit., p.108.

21 Ibid., p.198-199.

22 U.S. Congress. House. Committee on Science and Technology. Subcommittee on Transportation, Aviation and Materials. Computer and Communications Security and Privacy. Report April 1984. Washington, U.S. Government Printing Office, 1984. p.41.

23 The Members of the Committee include representations of the Attorney General, Secretaries of Commerce and Defense, Chairman of the Federal Communications Commission, Director of the Federal Bureau of Investigation, and Secretary of the Treasury.

24 IDA Paper P-1788. DoD Related Software Technology Requirements, Practices, and Prospects for the Future. Authored by Samuel T. Redwine, Jr., (et.al) (Unclassified), June 1984.

APPENDIX A

GLOSSARY OF TECHNICAL TERMS*

*Source: U.S. Department of Justice, Bureau of Statistics, Computer Crime: Criminal Justice Resource Manual, Washington, 1980.

GLOSSARY OF TECHNICAL TERMS

This glossary provides, in layman's terms, the contemporary meanings of the specialized data processing terms used in this manual. The glossary may be used as an independent source of information to clarify terms the prosecutor encounters both in investigation and in court. Where useful, definitions have been extracted from other recognized glossaries and computer crime legislation. The prosecutor can readily note that a definition is from a computer crime law or bill because it is enclosed in quotation marks. The numbers following some definitions refer to the source, as is listed below.

The entries are arranged in alphabetical order; special characters and spaces between words are ignored. Acronyms are placed in the same sequence as other terms, according to their spelling. When two or more terms have the same meaning, definitions are given only under the preferred term. Other relationships between terms are set forth at the end of the definition, as are cross references. Upper case terms in definitions refer to terms also defined in the glossary.

APPLICATION PROGRAM: A COMPUTER PROGRAM, written for or by a computer user, that causes a COMPUTER SYSTEM to satisfy his purposes.

APPLICATIONS PROGRAMMER: One who designs, develops, DEBUGS, installs, maintains, and documents APPLICATION PROGRAMS.

ASSEMBLER: A COMPUTER PROGRAM that translates COMPUTER PROGRAM instructions written in ASSEMBLY LANGUAGE into MACHINE LANGUAGE.

ASSEMBLY LANGUAGE: A SOURCE LANGUAGE that includes symbolic MACHINE LANGUAGE statements in which there is a one-to-one correspondence with the instructions in the form of MACHINE LANGUAGE of the computer.

ASYNCHRONOUS ATTACKS: Taking advantage of the asynchronous nature of computer OPERATING SYSTEMS to perpetrate an unauthorized act, e.g., confusing the queuing of jobs awaiting servicing.

AUDIT TRAIL: A sequential record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

BASIC (Beginners All-Purpose Symbolic Instruction Code): An algebra-like computer programming language used for problem-solving by engineers, scientists, and others who may not be professional PROGRAMMERS. Designers of the language intended that it should be a simplified derivative of FORTRAN.

BATCH PROCESSING: The processing of DATA or the accomplishment of jobs accumulated in advance in such a manner that each accumulation thus formed is processed or accomplished in the same computer run.

BIT (BInary digiT):

(1) In the binary numeration system, either of the digits 0 or 1.

(2) An element of DATA that takes either of two states or values.

BYTE: A sequence of usually 6 or 8 BITS operated upon as a unit and often part of a computer WORD. This sequence may represent a character.

CHECKPOINT RESTART: A point in time or processing sequence in a machine run at which processing is momentarily halted to make a record of the condition of all the variables of the machine run, such as the position of input and output (I/O) tapes and a copy of the contents of working storage. This process, in conjunction with a restart routine, minimizes reprocessing time occasioned by machine or other failures.

COBOL (COmmon Business-Oriented Language): A HIGH-LEVEL computer programming language designed for business data processing.

COM (Computer Output Microfilm):

(1) Microfilm that contains DATA that are received directly from computer-generated signals.

(2) To place computer-generated DATA on microfilm.

(3) A recording device that produces computer output microfilm.

COMMUNICATIONS ENGINEER/OPERATOR: One who operates communications equipment including concentrators, multiplexors, modems, and line switching units. Ordinarily, this person reconfigures the communications network when failures or overload situations occur.

COMPILER: A COMPUTER PROGRAM used to translate a COMPUTER PROGRAM expressed in a problem-oriented language (SOURCE CODE) into MACHINE LANGUAGE (OBJECT CODE).

COMPUTATION BOUND: The state of execution of a COMPUTER PROGRAM in which the computer time for execution is determined by computation activity rather than I/O activity.

Contrast with: I/O BOUND

COMPUTER:

(1) "...an internally programmed, automatic device that performs data processing." [1]

(2) "...an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network." [2]

(3) "...an electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network." [3]

COMPUTER ABUSE: Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain.

COMPUTER CRIME (See COMPUTER-RELATED CRIME)

COMPUTER NETWORK:

(1) "...a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities. [1]

(2) "...the interconnection of communications lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers." [2]

(3) "...an interconnection of two or more computer systems." [4]

COMPUTER OPERATOR: A person who operates a computer, including duties of monitoring system activities, coordination of tasks, and the operation of equipment.

COMPUTER PROGRAM:

(1) "...an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data." [1]

(2) "...a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer in a manner designed to provide appropriate products from such computer system." [2]

(3) "...an ordered set of instructions or statements, and related data, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions." [4]

COMPUTER-RELATED CRIME: Any illegal act for which knowledge of computer technology is essential for successful prosecution.

COMPUTER SECURITY SPECIALIST: A person who evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls that are related to the use of COMPUTER SYSTEMS.

COMPUTER SYSTEM:

(1) "...a set of related, connected or unconnected computer equipment, devices, or computer software." [1]

(2) "...a machine or collection of machines, used for governmental, educational, or commercial purposes, one or more of which contain computer programs and data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." [4]

CPU (Central Processing Unit): The device in a COMPUTER SYSTEM that includes the circuits controlling the interpretation and execution of instructions. The term may also refer to the portion of the computer that contains its control, logic, and sometimes internal storage.

CRT (Cathode Ray Tube): A device that presents DATA or graphics in visual form by means of controlled electron beams. This electronic vacuum tube is much like a television picture tube.

DATA:

(1) DATA are a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automatic means. DATA may be representations, such as characters or analog quantities, to which meaning is, or might be, assigned.

(2) DATA may be defined as any representation of fact or idea in a form that is capable of being communicated or manipulated by some process.

(3) "...a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network." [4]

Contrast with: INFORMATION

DATA BASE: An organized collection of DATA processed and stored in a COMPUTER SYSTEM.

DATA BASE ADMINISTRATOR: An individual with an overview of one or more DATA BASES, who controls the design and use of these DATA BASES. Responsiblities are the addition, modification, and deletion of records and frequently the security of the DATA BASE.

DATA COMMUNICATIONS: The transmission, reception, and validation of DATA.

DATA DIDDLING: The unauthorized changing of DATA before or during their input to a COMPUTER SYSTEM. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards for prepared replacements.

DATA ENTRY AND UPDATE CLERK: A person who adds, changes, and deletes records in computer-stored DATA BASES by means of a computer terminal, or manually updates punch cards or entries on input data forms for computer input.

DATA LEAKAGE: Unauthorized, covert removal or obtaining copies of DATA from a COMPUTER SYSTEM, e.g., sensitive DATA may be hidden in otherwise innocuous looking reports. This is a deliberate act whereas DATA seepage, the provision of DATA or information to unauthorized individuals, is accidental.

DATA SET (See FILE)

DBMS (Data Base Management System): A computer APPLICATION PROGRAM or set of programs that provides STORAGE, retrieval, updating, management, and maintenance of one or more DATA BASES.

DDA (Deputy District Attorney): An assistant to a District Attorney.

DEBUG: To detect, locate, and remove mistakes or malfunctions from a COMPUTER PROGRAM or COMPUTER SYSTEM.

DIRECT ACCESS: A method for the retrieval or storage of DATA, by reference to their addressable location in a STORAGE device, rather than to their location by position in a sequence.

Contrast with: SEQUENTIAL ACCESS

DISTRIBUTED PROCESSING: Electronic data processing (EDP) performed in computers near or at the sources of data and/or near the users of results where the data processing might otherwise be performed at a single, central site removed from data sources or users.

EDP (Electronic Data Processing) AUDITOR: A person who performs operational, computer, COMPUTER PROGRAM, and data file reviews to determine integrity, adequacy, performance, security, and compliance with organization and generally accepted policies, procedures, and standards. This person also may participate in design specification of applications to ensure adequacy of controls; performs data processing services for auditors.

EFTS (Electronic Funds Transfer System): A computer and TELECOMMUNICATION network to execute a wide range of monetary transfers.

FACILITIES ENGINEER: A person who inspects, adjusts, repairs, modifies, or replaces equipment supporting computer and terminal facilities, e.g., air conditioning, light, heat, power, and water.

FILE A collection of related DATA records treated as a unit. For example, one line of an invoice may form an item, a complete invoice may form a record, the complete set of records may form a FILE.

Synonym: DATA SET

FIRMWARE (computer jargon, not recommended for use): A COMPUTER PROGRAM that is considered to be a part of a computer and not modifiable by computer OPERATING SYSTEM or APPLICATION PROGRAMS. It often makes use of computer instructions not available for normal programming. It is often called a microprogram. The name is derived from other jargon terms, SOFTWARE and HARDWARE.

FORTRAN (FORmula TRANslation): A higher level programming language primarily used to write COMPUTER PROGRAMS that tend to be more engineering- or scientific-oriented rather than business-oriented.

FRONT-END PROCESSOR: A special-purpose computer used to reduce the work load of the main computer primarily for input, output, and data communications functions.

HARDWARE (computer jargon, not recommended for use): The computer and all related or attached machinery, such as mechanical, magnetic, electrical, and electronic devices, used in data processing.

Contrast with: SOFTWARE

HIGH-LEVEL LANGUAGE: A programming language that is independent of the structure of any one given computer or that of any given class of computers. Some particular languages are designed for specialized applications.

Contrast with: ASSEMBLY LANGUAGE

INFORMATION: The meaning that a human assigns to DATA by means of conventions used in their representation.

See: DATA

INSTRUCTION: A statement appearing in a COMPUTER PROGRAM that specifies an operation and the values or locations of its operands.

INSTRUCTION LOCATION: The place or address where DATA in the form of an INSTRUCTION, may be stored within a COMPUTER SYSTEM.

INTERACTIVE: The mode of use of a COMPUTER SYSTEM in which each action external to the COMPUTER SYSTEM elicits a timely response. An interactive system may also be conversational, implying a continuous dialog between the user and the COMPUTER SYSTEM.

I/O BOUND: The state of execution of a COMPUTER PROGRAM in which the computer time for execution is determined by I/O activity rather than computation activity.

Contrast with: COMPUTATION BOUND

JCL (see JOB CONTROL LANGUAGE)

JOB: A set of DATA and COMPUTER PROGRAMS that completely define a unit of work for a computer. A job usually includes all necessary COMPUTER PROGRAMS, mechanisms for linking COMPUTER PROGRAMS, DATA, FILES, and INSTRUCTIONS to the OPERATING SYSTEM.

JOB CONTROL LANGUAGE: A programming language used to code job control statements. A job control program is a COMPUTER PROGRAM that is used by the COMPUTER SYSTEM to prepare each job or job step to be run.

JOB QUEUE: A sequenced set of JOBS in COMPUTER STORAGE arranged in order of assigned priority for execution by a computer.

JOB SETUP CLERK: A person who assembles jobs. This task includes compilation of DATA, COMPUTER PROGRAMS, and job control information. This person requests that JOBS be executed, requests media libraries for necessary DATA, physically places jobs and DATA into JOB QUEUES, handles procedures for reruns, and possibly distributes output to users.

LOAD AND GO: A computer operation method by which higher level language programs or JOBS are entered, prepared for execution, and immediately executed.

LOCAL PROCESSING: Data processing that is conducted near or at the user's location, rather than at a remote CPU.

LOGIC BOMBS: A COMPUTER PROGRAM residing in a computer that is executed at appropriate or periodic times to determine conditions or states of a COMPUTER SYSTEM and that facilitates the perpetration of an unauthorized act.

LOOP: A sequence of INSTRUCTIONS in a COMPUTER PROGRAM that is executed repeatedly until a terminal condition prevails.

MACHINE LANGUAGE: A computer programming language that is used directly by a computer, without having to pass through a translation program, such as a COMPILER.

MAIN STORAGE: The fastest access STORAGE device in a COMPUTER SYSTEM where the storage locations can be addressed by a COMPUTER PROGRAM, and INSTRUCTIONS and DATA can be moved from and into registers in the CPU from which the INSTRUCTIONS can be executed or from which the DATA can be operated upon.

MASTER FILE: A FILE of DATA that is used as an authority in a given JOb and that is relatively permanent, even though its contents may change from run to run.

MEDIA LIBRARIAN: A person who files, retrieves, and accounts for OFF-LINE storage of DATA on disk, tape, cards, or other removable data STORAGE media. The person provides media for the production control and job set-up areas and functions, and cycles backup files through remote STORAGE facilities.

MEDIUM: The material, or configuration thereof, on which DATA are recorded. Examples are punched paper tape, punch cards, magnetic tape, and disks.

MEMO UPDATE: A FILE update procedure whereby MASTER FILES are not directly modified to reflect each transaction. Instead, pointers to other files are used to keep track of updates to specified records. Pointers are used periodically to obtain the data to merge with and update a MASTER FILE.

MEMORY (See MAIN STORAGE)

MICR (Magnetic Ink Character Recognition): A standard machine-readable type font printed with magnetic ink on documents such as bank checks and deposit slips that can be directly read by machine.

MIS (Management Information System): An integrated man/machine COMPUTER SYSTEM for providing INFORMATION to support the operations, management, and decision-making functions in an organization. Ordinarily, the system utilizes management and decision models, and a DATA BASE.

MODEM (MOdulator-DEModulator): A device that modulates and demodulates signals transmitted over DATA TELECOMMUNICATION facilities. This transformation, i.e., conversion of digital signals to analog signals and back again, is necessary for use of common voice-grade telephone lines for COMPUTER communication purposes.

MULTIPROCESSING: The use of two or more CPUs in a COMPUTER SYSTEM under integrated control.

MULTIPROGRAMMING: The concurrent execution of two or more PROGRAMS accomplished by sharing the resources of a computer.

NETWORK (See COMPUTER NETWORK)

OBJECT CODE: Output from a COMPILER or ASSEMBLER that is executable MACHINE LANGUAGE.

Contrast with: SOURCE CODE

OCR (Optical Character Recognition): The machine identification of printed characters through use of light sensitive devices.

Contrast with: MICR

ON-LINE: The state of devices or computer users in direct communication with a CPU. Also a COMPUTER SYSTEM in an INTERACTIVE or TIME-SHARING mode with people or other processes.

Contrast: OFF-LINE

OPERATING SYSTEM: An integrated collection of COMPUTER PROGRAMS resident in a computer that supervise and administer the use of computer resources to execute jobs automatically.

OPERATIONS MANAGER: The manager of a computer facility responsible for the operation of the COMPUTER SYSTEM. He may also be responsible for the maintenance, specification, acquisition, modification, and replacement of COMPUTER SYSTEMS or COMPUTER PROGRAMS.

OPERATOR (See COMPUTER OPERATOR)

PERIPHERAL EQUIPMENT OPERATOR: A person who operates devices peripheral to the COMPUTER that performs DATA I/O functions.

PIGGYBACKING: A method of gaining unauthorized physical access to guarded areas when control is accomplished by electronically or mechanically locked doors. For example, a person may follow another through the doors although he does not possess the required authorization to pass. Electronic piggybacking occurs when a computer or terminal covertly shares the same communication line as an authorized user. The host computer, to which they both transmit, is unable to distinguish between those signals of the authorized and those of the unauthorized user.

PIN (Personal Identification Number): A password that must be entered by a COMPUTER SYSTEM user to gain access to a specific APPLICATIONS PROGRAM. Most often the term is associated with retail computer banking devices such as Automated Teller Machines (ATMs).

PL/1: A High-Level computer programming language designed for use in a wide range of business and scientific computer applications.

POS (POINT-OF-SALE) TERMINALS: Computer terminals used for transaction recording, credit authorization, and funds transfer and typically are situated within merchant establishments at the point of retail sales.

PRODUCTION PROGRAM: A PROGRAM which has been DEBUGGED and tested and is considered no longer in the development stage. Such a PROGRAM is often part of a library of programs used for data processing.

PROGRAM (See COMPUTER PROGRAM)

PROGRAMMER: A person who engages in designing, writing, and testing computer PROGRAMS.

PROGRAMMING MANAGER: A person who manages computer PROGRAMMERS to design, develop, and maintain computer programs.

REAL-TIME: The actual time during which a physical process transpires. Also a computer operation mode in which a computation takes place during the actual time that the related physical process transpires in order that results of the computation can be used in controlling and monitoring the physical process.

REMOTE JOB ENTRY (RJE): Submission of jobs through an input unit that has access to a computer through a DATA COMMUNICATIONS link.

REMOTE PROCESSING: Data entry and partial or complete processing near the point of origin of a transaction. Remote processing systems typically edit and prepare DATA input before transmission to a central computer.

ROM (Read-Only Memory): A semiconductor storage device in which the data content is fixed, readout is nondestructive, and DATA are retained indefinitely even when the power is shut off. In contrast, RAMs (Random-Access read/write Memories) are capable of read and write operations, have non-destructive readout, but stored DATA is lost when the power is shut off.

RPG (Report Program Generator): A High-Level computer programming language that is report-rather than procedure-oriented. PROGRAMMERS describe the functions desired of the computer by describing the output report.

RUN BOOK: A document containing INSTRUCTIONS for COMPUTER OPERATORS detailing operations set up procedures, job schedule checklists, action commands, error correction and recovery instructions, I/O dispositions, and system backup procedures.

SALAMI TECHNIQUES: The unauthorized, covert process of taking small amounts (slices) of money from many sources in and with the aid of a computer. An example is the round down fraud, whereby remainders from the computation of interest are moved to a favored account instead of being systematically distributed among accounts.

SCAVENGING: A covert, unauthorized method of obtaining information that may be left in or around a computer system after the execution of a JOB. Included here is physical search (trash barrels, carbon copies, etc.) and search for residual DATA within the computer STORAGE areas, temporary storage tapes, and the like).

SECURITY OFFICER: A person who evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls.

SEQUENTIAL ACCESS: An access method for storing or retrieving DATA according to their sequential order in a STORAGE device.

Contrast with: DIRECT ACCESS

SIMULATION AND MODELING IN A CRIME: The use of a computer as a tool for planning or controlling a crime. An instance of this would be the simulation of an existing process to determine the possibility of success of a premeditated crime.

SOFTWARE ~~(Jargon~~, not recommended for use): "Computer Software means a set of computer programs, procedures, and associated documentation concerning the operation of a computer system." [1]

Contrast with: COMPUTER PROGRAMS, OPERATING SYSTEM

SOURCE CODE: INSTRUCTIONS in a computer programming language that are used as input for a COMPILER, interpreter, or ASSEMBLER.

Contrast with: OBJECT CODE

SPOOLING: The reading and writing of DATA for I/O on auxiliary STORAGE devices, concurrently with execution of other jobs, in a format for later processing or output operations.

STORAGE:

(1) The action of placing DATA into a STORAGE device and retaining them for subsequent use.

(2) A device used for retaining DATA or COMPUTER PROGRAMS in machine-readable and retrievable form.

STORAGE CAPACITY: The number of BITS, characters, BYTES, WORDS, or other units of DATA that a particular STORAGE device can contain.

SUPERZAPPING: The unauthorized use of utility COMPUTER PROGRAMS that violate computer access controls to modify, destroy or expose DATA in a computer. The name derives from an IBM utility program called "Superzap."

SYSTEM (See COMPUTER SYSTEM)

SYSTEM ENGINEER: A person who designs, configures, tests, diagnoses, assembles and disassembles, and repairs or replaces COMPUTER SYSTEM devices and components.

SYSTEMS PROGRAMMER: A person who designs, develops, installs, modifies, documents, and maintains OPERATING SYSTEM and utility programs.

TELEPROCESSING: The processing of DATA that are received from or sent to remote locations by way of telecommunication circuits.

TELEPROCESSING MONITOR: A computer OPERATING SYSTEM program that controls the transfer of DATA between the communication circuits and a computer and often does the user polling (turn-taking among users) as well.

TERMINAL ENGINEER: A person who tests, diagnoses, assembles and disassembles, repairs, and replaces terminals or their components.

TIME-SHARING: A method of using a computing system that allows a number of users to execute programs concurrently and to interact with the programs during execution. A time-shared computer is used by several users at once.

Related term: BATCH PROCESSING

TRANSACTION OPERATOR: A person who operates a computer transaction terminal by entering transactions for processing by a COMPUTER SYSTEM. An example of such a device would be a POS TERMINAL.

TRANSACTION SYSTEM: A COMPUTER SYSTEM that is used for processing transactions in a prescribed manner controlled by APPLICATION PROGRAMS.

TRAP DOOR: A function, capability, or error in a COMPUTER PROGRAM that facilitates compromise or unauthorized acts in a COMPUTER SYSTEM.

TROJAN HORSE: Computer INSTRUCTIONS secretly inserted in a COMPUTER PROGRAM so that when it is executed in a computer unauthorized acts are performed.

UPDATE-IN-PLACE: A method for the modification of a MASTER FILE with current DATA each time a transaction is received in a COMPUTER SYSTEM.

Contrast with: MEMO UPDATE

UTILITY PROGRAM: A COMPUTER PROGRAM designed to perform a commonly used function, such as moving DATA from one STORAGE device to another.

WIRETAPPING: Interception of DATA COMMUNICATIONS signals with the intent to gain access to DATA transmitted over communications circuits.

WORD: A sequence of adjacent characters or BITS considered as an entity in a COMPUTER.

APPENDIX B

COMPUTER ABUSE
SELECTED BIBLIOGRAPHY
1976-1984

Prepared by E. Ann Sarles
and James T. Higgins

IDA-Technical Information Services

COMPUTER ABUSE

SELECTED BIBLIOGRAPHY 1976-1984

Preface

This bibliography has been prepared to supplement the information provided in this paper. the intent is to provide the reader with bibliographic sources relating to the topic of computer crime and the need for federal legislation in this area.

The cited articles and monographs have for the most part been selected from the computerized data base maintained by the National Criminal Justice Reference Service. Other sources searched for additional information include commercial data bases, government reports and the Library of Congress Legal Division. Louise Becker provided invaluable assistance in the selection of materials from the vast number of items published on computer-related crime.

E. Ann Sarles
James T. Higgins
Research Librarians
Technical Information Services
15 Aug 1984

"Addressing Computer Crime Legislation: Progress and Regress." Computer Law Journal, v IV, n 1 Summer 1983, p. 195-206.

American Bar Association. Report on Computer Crime. Task Force on Computer Crime Section of Criminal Justice, 1984. various pagings.

Becker, J. "Trial of a Computer Crime." Prosecutor, v 16, n 2 Winter 1982, p. 23-29.

Bentley, S. W. "Model Training Program in Computer Investigations for Law Enforcement Investigations." Law Enforcement Data Processing Symposium - Fifth Annual, 1981, p. 205-218.

Bequai, A. How to Prevent Computer Crime - A Guide for Managers. Somerset, NJ, Wiley, 1983. 321p.

----- "Why We Need Computer Legislation." Interactive Computing, v 6, n 4 July/August 1980, p. 4-8.

Burgess, John. " Computer Crime: Peril of Progress." Trial, v 17, n 1 Jan 1981, p. 6-8.

"Computer Crime." American Criminal Law Review, v 18 Fall 1980, p. 370-386.

Couch, R. M. " Suggested Legislative Approach to the Problem of Computer Crime." Washington and Lee Law Review, v 38, n 4 Fall 1981, p. 1173-1194.

Fleming, Alexander F. "Recent Statutes." Suffolk University Law Review, v XIV, n 826 1980, p. 832-840.

Freese, J. Swedish Data Act. Swedish Institute, S-103 82 Stockholm, Sweden, 1977.

Gammer, M. A. "Computer Crime." American Criminal Law Review, v 18, n 2 Fall 1980, p. 370-386.

Glynn, Elizabeth A. "Computer Abuse: The Emerging Crime and the Need for Legislation." Fordham Urban Law Journal, v 12 Winter 1983-1984, p. 73-101.

Kennedy, Neal R. "A Look at Computer Crime - Oklahoma and Federal Law." The Oklahoma Bar Journal, v 54, n 49, p. 3263-3274.

Kling, Rob. "Computer Abuse and Computer Crime as Organizational Activities." Computer Law Journal, v II, n 2 Spring 1980, p. 403-427.

"Lawmakers Tackle Computer Crime." Trial, v 20, n 2 Feb 1984, p. 8.

Lenart, John N. "Computer Fraud: A Legal Challenge." New Zealand Law Journal, Sept 1983, p. 273-278.

Levy, Robert B. "Criminal Liability for Computer Offenses and the New Wisconsin Computer Crimes Act." Wisconsin Bar Bulletin, March 1983, p. 21-23+

McNiff, F. V. Criminal Liability for Australian Computer Abuse. Institute of Caulfield, Victoria 3145, Australia, 1980, 86p.

Myers, John. "Fraud and Computers." New Law Journal, v 133, n 6087 Jan 21, 1983, p. 71-72.

Nocera, J. A. and J. W. Lovelace. "Strengthening Fraud Detection The DCAA (Defense Contract Audit Agency) View." Internal Auditor, v 37, n 2 April 1980, p. 23-29.

Norman, Adrian R. D. Computer Insecurity. New York, Chapman and Hall, 1983.

Parker, D. B. Fighting Computer Crime. New York, Scribner, 1983. 357p.

Quinn, Frank X. "Computer Crime: Computer Abuse as a Basis for Criminal Liability." New Zealand Law Journal, Sept 1983, p. 270-173.

Roddy, John. "The Federal Computer Systems Protection Act." Journal of Computers, Technology and Law, v 7 1980, p. 343-365.

Rose, Frank. "Joy of Hacking." Science 82, v 3 Nov 1982, p. 59-66.

Schjolberg, Stein, "Computer-Assisted Crime in Scandinavia." Computer Law Journal, V II, n 2 Spring 1980, p. 352-382.

----- Computers and Penal Legislation - A Study of the Legal Politics of a New Technology. Norwegian Research Center for Computers and Law, University of Oslo, Oslo, Norway, 1983, 155p.

Sokolik, Stanley, L. "Computer Crime - The Need for Deterrent Legislation." Computer Law Journal, v II n 2 Spring 1980, P. 353-383.

Steel, G. T. and A. L. Pearson. Case for Training in Computer Crime Investigation. Law Enforcement Data Processing Symposium - Fifth Annual, 1981, p. 219-231.

U.S. Congress. House. Committee on Science and Technology. Subcommittee on Transportation, Aviation and Materials. Computer and Communication Security and Privacy. Hearing, 98th Congress 1st Session. Washington, U.S. Govt., Print. Off., 1983.

----- Committee on the Judiciary. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Washington, U.S. govt. Print. Off., 1984.

----- Committee on the Judiciary. Subcommittee on Civil and Consititutional Rights. Federal Computer Systems Protection Act. Hearing, 97th Congress 2d Session. Washington, U.S. Govt., Print. Off., 1984.

U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on Oversight of Governmental Management. Computer Security in the Federal Government and the Private Sector. Hearing. 98th Contress 1st Session. Washington, U.S. Govt. Print. Off., 1983.

----- Committee on Governmental Affairs. Permanent Subcommittee on Investigation. Federal Computer Security: An Analysis of Congressional Initiatives and Executive Branch Responsibilities. Prepared by the Congressional Research Service, U.S. Library of Congress. Washington, U.S. Govt. Print. Off., 1983.

----- Committee on Government Operations. Computer Security in Federal Programs. Washington, U.S. Govt. Print. Off., 1977.

----- Committee on Government Operations. Problems Associated with Computer Technology in Federal Programs and Private Industry: Computer Abuses. Washington, U.S. Govt. Print. Off., 1976.

----- Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. Federal Computer Systems Protection Act. 95th Congress 2d Session. Hearings on S 1766. Washington, U.S. Govt. Print. Off., 1979.

----- Committee on the Judiciary. Subcommittee on Criminal Justice. Computer Systems Protection Act of 1979, S 240. 96th Congress 2d Session. Washington, U.S. Govt. Print. Off., 1980.

U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime: Criminal Justice Resource Manual. Washington, U.S. Govt. Print. Off., 1979. 329p.

----- Computer Crime: Legislative Resource Manual. Washington, U.S. Govt. Print. Off., 1980. 66p.

----- Computer Crime: Expert Witness Manual. Washington, U.S. Govt, Print. Off., 1980. 28p.

----- Computer Crime: Electronic Fund Transfer Systems and Crime. Washington, U.S. Govt. Print. Off., 1982. 182p.

----- Computer Crime: Computer Security Techniques. Washington, U.S. Govt. Print. Off., 1982. various pagings.

U.S. General Accounting Office. Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices. April 21, 1982, MASAD-82-81. Washington, U.S. General Accounting Office, 1982. 29p.

----- Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies. Nov 12, 1980, LCD-81-1. Washington, U.S. General Accounting Office, 1980. 69p.

U.S. Library of Congress. Congressional Research Service. Computer Security: An Overview of National Concerns and Challenges. Feb 3, 1983 (by) Louise G. Becker, Specialist in Information Science and Technology, Science Policy Research Division. (Multilith no. 83-135 SPRD) Washington, 1983. 241p.

----- Unauthorized Reception of Communications Satellite Signals Carrying Video Programs. Aug 6, 1984 (by) David r. Siddall, Legislative Attorney, American Law Division. Washington, 1984. 97p.

U.S. Office of Technology Assessment. Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity. Washington, 1982. 77p. (Background Paper)

U.S. President's Council on Integrity & Efficiency and President's Council on Management Improvement. Computer Security Seminar - Proceedings. Held at Bethesda, MD. Washington, 1984. various pagings.

Watts, J. R. Computer-Related Fraud - Current Issues and Directions. U.S. General Accounting Office, Accounting and Financial Management Division, Washington, 1981. 20p.

Wharton, Leslie. "Comment: Legislative Issues in Computer Crime." Harvard Journal on Legislation, v 21, n 1 Winter 1984, p. 239-254.

"White-Collar Crime - A Survey of Law." American Criminal Law Review, V 18, n 2 Fall 1980. (Complete Issue)

APPENDIX C

Federal Legislative Measures

CHAPTER XXI—ACCESS DEVICES AND COMPUTERS

SEC. 2101. This chapter may be cited as the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984".

SEC. 2102. (a) Chapter 47 of title 18 of the United States Code as amended by chapter XVI of this joint resolution is further amended by adding at the end thereof the following:

"§ 1030. Fraud and related activity in connection with computers

"(a) Whoever—

"(1) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

"(2) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the oppor-

* Enrolled bill, H.J. Res 648

tunity such access provides for purposes to which such authorization does not extend, and thereby obtains information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

"(3) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;

shall be punished as provided in subsection (c) of this section. It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.

"(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

"(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

"(c) The punishment for an offense under subsection (a) or (b)(1) of this section is—

"(1)(A) a fine of not more than the greater of $10,000 or twice the value obtained by the offense or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine of not more than the greater of $100,000 or twice the value obtained by the offense or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(2)(A) a fine of not more than the greater of $5,000 or twice the value obtained or loss created by the offense or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(B) a fine of not more than the greater of $10,000 or twice the value obtained or loss created by the offense or imprisonment for not than ten years, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which occurs after

a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

"(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

"(e) As used in this section, the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.".

(b) The table of sections at the beginning of chapter 47 of title 18 of the United States Code is amended by adding at the end the following new items:

"1030. Fraud and related activity in connection with computers.".

SEC. 2103. The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution, concerning prosecutions under the sections of title 18 of the United States Code added by this chapter.

98TH CONGRESS
1ST SESSION

H. R. 1092

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 31, 1983

Mr. NELSON of Florida introduced the following bill; which was referred to the Committee on the Judiciary

NOVEMBER 16, 1983

Additional sponsors: Mr. BENNETT, Mr. FORSYTHE, Mr. HALL of Ohio, Mr. LAFALCE, Mr. PRICE, Mr. WILLIAMS of Montana, Mr. WON PAT, Mr. BEVILL, Mr. DWYER of New Jersey, Mr. FASCELL, Mr. SENSENBRENNER, Mr. SMITH of Florida, Mr. ADDABBO, Mr. CORRADA, Mr. LAGOMARSINO, Mr. VANDERGRIFF, Mr. WHITLEY, Mr. BARNARD, Mr. LEWIS of Florida, Mr. MCCOLLUM, Mr. FRENZEL, Mr. HORTON, Mr. OXLEY, Mr. RINALDO, Mr. SMITH of New Jersey, Mr. WASHINGTON, Mr. ROE, Mr. GOODLING, Mr. HUTTO, Mr. SUNIA, Mr. WINN, Mr. ENGLISH, Mr. DYMALLY, Mr. ORTIZ, Mr. MACKAY, Mr. FROST, Mr. PATMAN, Mr. HEFTEL of Hawaii, Mr. MCDADE, Mr. WILLIAMS of Ohio, Mr. GILMAN, Mr. LENT, Mr. IRELAND, Mr. YOUNG of Florida, Mr. MCNULTY, Mr. LEATH of Texas, Mr. EDWARDS of Oklahoma, Mr. LONG of Louisiana, Mr. GORE, Mr. HEFNER, Mr. JENKINS, Mr. MICA, Mr. MURPHY, Mr. MOAKLEY, Mr. FORD of Tennessee, Mr. RATCHFORD, Mr. NIELSON of Utah, Mr. FUQUA, Mr. KINDNESS, Mr. SKELTON, Mr. DYSON, Mr. BILIRAKIS, Mr. DUNCAN, Mr. PHILIP M. CRANE, Mr. GLICKMAN, Mr. BRITT, Mr. MCCURDY, Mr. RUDD, Mr. STENHOLM, Mr. STOKES, Mr. SIMON, Mr. WORTLEY, Mr. STANGELAND, Mr. WHITEHURST, Mr. WILSON, Mr. MILLER of Ohio, Mr. ANDERSON, Mr. BONKER, Mr. KASICH, Mr. CLINGER, Mr. LANTOS, Mrs. SCHNEIDER, Mr. LOWERY of California, Mr. MINETA, Mr. GONZALEZ, Mr. CORCORAN, Mr. SCHAEFER, Mr. COELHO, Mr. YOUNG of Missouri, Mr. TORRICELLI, Mr. ANTHONY, Mr. ANDREWS of Texas, Mr. BROWN of California, Mr. WALKER, Mr. ROBINSON, Mr. QUILLEN, Mr. BATEMAN, Mr. LUKEN, Mr. BADHAM, Mr. CHANDLER, Mr. FIELDS, Mr. HYDE, Mr. RAHALL, Mr. WOLPE, Mrs. LLOYD, Mr. CONTE, Mr. MCKINNEY, Mr. MCCANDLESS, Mr. SYNAR, Ms. SNOWE, Mr. COUGHLIN, Mrs. HALL of Indiana, and Mr. DEWINE

A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1983".

SEC. 2. The Congress finds that—

(1) computer-related crime is a growing problem in the Government and in the private sector;

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) the opportunities for computer-related crimes in Federal programs, in financial institutions, and in computers which operate in or use a facility of interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of comput-

erized information files, and stealing of financial instruments, data, or other assets, are great;

(4) computer-related crime directed at computers which operate in or use a facility of interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer-related crime is difficult under current Federal criminal statutes.

SEC. 3. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse

"(a) Whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or knowingly convert to his use or the use of another, the property of another, shall, if the computer—

"(1) is owned by, under contract to, or operated for or on behalf of:

"(A) the United States Government; or

"(B) a financial institution;

and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or a financial institution; or

"(2) operates in, or uses a facility of, interstate commerce;

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever intentionally and without authorization damages a computer described in subsection (a) or intentionally and without authorization causes or attempts to cause the withholding or denial of the use of a computer, a computer program or stored information shall be fined not more than $50,000 or imprisoned not more than five years or both.

"(c) DEFINITIONS.—For the purpose of this section the term—

"(1) 'computer' means an electronic, magnetic, optical, hydraulic, organic or other high speed data processing device or system performing logical, arithmetic, or storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system; but does not include an automated typewriter or typesetter, a portable hand-held calculator, or any computer designed and manufactured for, and which is used exclusively for, routine personal, family, or household purposes and which is not used to access,

to communicate with, or to manipulate any other computer;

"(2) 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(3) 'property' means anything of value, and includes tangible and intangible personal property; information in the form of computer processed, produced, or stored data; information configured for use in a computer; information in a computer medium; information

being processed, transmitted or stored; computer operating or applications programs; or services;

"(4) 'services' includes computer data processing and storage functions;

"(5) 'United States Government' includes a branch or agency thereof; and

"(6) 'use' includes to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer, or, with fraudulent or malicious intent, to cause another to put false information into a computer; and

"(7) 'computer medium' includes the means of effecting or conveying data for processing in a computer, or a substance or surrounding medium which is the means of transmission of a force or effect that represents data for processing in a computer, or a channel of communication of data for processing in a computer.

"(d)(1) In a case in which Federal jurisdiction over an offense as described in this section exists concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation.

"(2) In a case in which Federal jurisdiction over an offense as described in this section exists or may exist concur-

rently with State or local jurisdiction, Federal law enforcement officers, in determining whether to exercise jurisdiction, shall consider—

"(A) the relative gravity of the Federal offense and the State or local offense;

"(B) the relative interest in Federal investigation or prosecution;

"(C) the resources available to the Federal authorities and the State or local authorities;

"(D) the traditional role of the Federal authorities and the State or local authorities with respect to the offense;

"(E) the interests of federalism; and

"(F) any other relevant factor.

"(3) The Attorney General shall—

"(A) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in cases in which Federal jurisdiction as described in this section exists or may exist concurrently with State or local jurisdiction;

"(B) provide general direction to Federal law enforcement officers concerning the appropriate exercise of such Federal jurisdiction which, for the purposes of investigation, is vested concurrently in the Department of Justice and the Department of the Treasury;

"(C) report annually to Congress concerning the extent of the exercise of such Federal jurisdiction during the preceding fiscal year; and

"(D) report to Congress, within one year of the effective date of this Act, on the long-term impact upon Federal jurisdiction, of this Act and, the increasingly pervasive and widespread use of computers in the United States. The Attorney General shall periodically review and update such report.

"(4) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of Federal jurisdiction may be made available to State or local law enforcement officers having concurrent jurisdiction, and to State or local authorities otherwise assigned responsibility with regard to the conduct constituting the offense.

"(5) An issue relating to the propriety of the exercise of or of the failure to exercise Federal jurisdiction over an offense as described in this section, or otherwise relating to the compliance, or to the failure to comply, with this section, may not be litigated, and a court may not entertain or resolve such an issue except as may be necessary in the course of granting leave to file a dismissal of an indictment, an information, or a complaint.".

SEC. 4. The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse.".

O

II

98TH CONGRESS
2D SESSION

S. 2270

To amend title 18 of the United States Code to prohibit the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 8 (legislative day, FEBRUARY 6), 1984

Mr. COHEN (for himself, Mr. LEVIN, and Mr. RUDMAN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To amend title 18 of the United States Code to prohibit the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Computer Crime Prevention Act of 1984."

SEC. 2. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse

"(a) Whoever, knowingly, intentionally, and without authorization, directly or indirectly uses, or attempts to use any computer for the purpose of—

"(1) devising or executing any scheme or artifice to defraud, or

"(2) obtaining money, property, or services, for themselves or another, by means of false or fradulent pretenses, representations, or promises,

shall, if the computer—

"(A) is owned by, under contract to, or operated for or on behalf of the United States Government or a financial institution, and the prohibited conduct directly involves or affects the computer operation for or on behalf of the United States Government or a financial institution; or

"(B) operates in, or uses a facility of, interstate commerce,

be fined not more than three times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever knowingly, intentionally, and without authorization damages or destroys or attempts to damage or destroy a computer described in subsection (a) or knowingly, intentionally, and without authorization alters or deletes or

attempts to alter or delete any computer program or data stored in a computer described in subsection (a) shall be fined not more than three times the amount of the loss directly or indirectly sustained from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(c) Whoever knowingly, intentionally, and without authorization buys, procures, or sells the password or access code for a computer described in subsection (a), for the purpose of—

"(1) devising or executing any scheme or artifice to defraud, or

"(2) obtaining money, property, or services, for themselves or another, by means of false or fraudulent pretenses, representations, or promises,

shall be fined not more than three times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(d) Whoever knowingly, intentionally, and without authorization uses a computer described in subs tion (a) shall be fined not more than $5,000 or imprisoned not more than one year, or both.

"(e) For the purpose of this section the term—

"(1) 'computer' means an electronic, magnetic, optical, hydraulic, organic, or other high-speed data

processing device or system performing logical, arithmetic, or storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system; but does not include an automated typewriter or typesetter, a portable hand-held calculator, or any computer designed and manufactured for, and which is used exclusively for, routine personal, family, or household purposes and which is not used to access, to communicate with, or to manipulate any other computer;

"(2) 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(3) 'property' means anything of value, and includes tangible and intangible personal property; information in the form of computer processed, produced, or stored data; information configured for use in a computer; information in a computer medium; information being processed, transmitted, or stored; computer operating or applications programs; or services;

"(4) 'services' includes computer data processing and storage functions;

"(5) 'United States Government' includes a branch or agency thereof; and

"(6) 'use' includes to access, instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer, or, with fraudulent or malicious intent, to cause another to put false information into a computer; and

"(7) 'computer medium' includes the means of effecting or conveying data for processing in a computer, or a substance or surrounding medium which is the means of transmission of a force or effect that repre-

sents data for processing in a computer, or a channel of communication of data for processing in a computer.

"(f)(1) In a case in which Federal jurisdiction over an offense as described in this section exists concurrently with State or local jurisdiction, the existence of Federal jurisdiction does not, in itself, require the exercise of Federal jurisdiction, nor does the initial exercise of Federal jurisdiction preclude its discontinuation.

"(2) In a case in which Federal jurisdiction over an offense as described in this section exists or may exist concurrently with State or local jurisdiction, Federal law enforcement officers, in determining whether to exercise jurisdiction, shall consider—

"(A) the relative gravity of the Federal offense and the State or local offense;

"(B) the relative interest in Federal investigation or prosecution;

"(C) the resources available to the Federal authorities and the State or local authorities;

"(D) the traditional role of the Federal authorities and the State or local authorities with respect to the offense;

"(E) the interests of federalism; and

"(F) any other relevant factor.

"(3) The Attorney General shall—

"(A) consult periodically with representatives of State and local governments concerning the exercise of jurisdiction in cases in which Federal jurisdiction as described in this section exists or may exist concurrently with State or local jurisdiction;

"(B) provide general direction to Federal law enforcement officers concerning the appropriate exercise of such Federal jurisdiction which, for the purposes of investigation, is vested concurrently in the Department of Justice and the Department of the Treasury; and

"(C) report annually to Congress concerning the extent of the exercise of such Federal jurisdiction during the preceding fiscal year.

"(4) Except as otherwise prohibited by law, information or material obtained pursuant to the exercise of Federal jurisdiction may be made available to State or local law enforcement officers having concurrent jurisdiction, and to State or local authorities otherwise assigned responsibility with regard to the conduct constituting the offense.

"(5) An issue relating to the propriety of the exercise of or of the failure to exercise Federal jurisdiction over an offense as described in this section, or otherwise relating to the compliance, or to the failure to comply, with this section, may not be litigated, and a court may not entertain or resolve such an issue except as may be necessary in the course of

granting leave to file a dismissal of an indictment, an information, or a complaint.".

SEC. 3. The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse.".

○

98TH CONGRESS
2D SESSION

S. 2940

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and other computers where the offense involves interstate or foreign commerce.

IN THE SENATE OF THE UNITED STATES

AUGUST 9, (legislative day, AUGUST 6), 1984

MR. THURMOND (by request) introduced the following bill; which was read twice and referred to the Committee on the Judiciary.

A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and other computers where the offense involves interstate or foreign commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1984".

SEC. 2. (a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§ 1028. Computer fraud and abuse

"(a) Whoever having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or convert to his use or the use of another, property not his own, for the purpose of executing such scheme or artifice or embezzlement, theft, or conversion, or attempting to do so, knowingly accesses or attempts to access a computer, shall—

"(1) if the computer is owned by, under contract to, or operated for or on behalf of—

"(A) the United States Government; or

"(B) a financial institution; or

"(2) if in committing or concealing the offense two or more computers are used which are located in different States or in a State and a foreign country;

be fined not more than two times the amount of the gain directly or indirectly derived from the offense or $50,000, whichever is higher, or imprisoned not more than five years, or both.

"(b) Whoever knowingly and willfully without authorization damages, destroys, or attempts to damage or destroy a computer described in subsection (a) (1) and (2) or knowingly and willfully without authorization damages or attempts to damage any computer program, or data contained in such

computer shall be fined not more than $50,000 or imprisoned not more than five years, or both.

"(c) Whoever intentionally and without authorization accesses a computer as defined in (a)(1), or a computer system or computer network including such computer, shall be guilty of a misdemeanor and shall be fined not more than $25,000 or imprisoned for not more than one year, or both.

"(d) Whoever violates any provision of paragraph (a), (b), or (c) shall forfeit to the United States any interest acquired or maintained in any computer and computer software, which has been used to commit the violation. Upon conviction under this section, the court shall authorize the Attorney General to seize all property or other interest declared forfeited under this section upon such terms and conditions as the court shall deem proper. If a property right or other interest is not exercisable or transferable for value by the United States, it shall expire, and shall not revert to the convicted violator. The United States shall dispose of all such property as soon as commercially feasible, making due provision for the rights of innocent persons.

"(e) The Attorney General is authorized to delegate, in whole or in part, to other departments and agencies concurrent investigative authority under this section subject to agreement between the Attorney General and the department or agency affected.

"(f) DEFINITIONS.—For the purpose of this section the term—

"(1) 'computer' means an electronic, magnetic, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"(2) 'computer system' means a set of related connected or unconnected computers, computer equipment, devices, and software;

"(3) 'computer network' means two or more interconnected computers, computer terminals, or computer systems;

"(4) 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal Home Loan Bank System and any home loan bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934;

"(5) 'property' includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer program and computer software in either machine or human readable form, computer services, and any other tangible or intangible item of value;

"(6) 'financial instrument' means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card or marketable security, or any electronic data processing representation thereof;

"(7) 'computer program' means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

"(8) 'computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

"(9) 'computer services' includes but is not limited to computer time, data processing, and storage functions;

"(10) 'United States Government' includes a branch or agency thereof; and

"(11) 'access' means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.".

SEC. 3. The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. Computer fraud and abuse.".

O

APPENDIX D

CITATIONS ON KEY STATE STATUTES ON COMPUTER CRIME

CITATIONS OF KEY STATE STATUTES ON COMPUTER CRIME

1. Alaska: Alaska Stat. § 11.46.985.
2. Arizona: Ariz. Rev. Stat. §§ 13-2301, 13-2316.
3. California: Cal. Penal Code § 502, 631.
4. Colorado: Colo. Rev. Stat. §§ 18-5.5-101, 18-5.5-102.
5. Connecticut: Public Act No. 84-206 (approved May 31, 1984).
6. Delaware: Del. Code Ann. tit. 11 §§ 858, 2738.
7. Florida: Fla. Stat. Ann. §§ 815.01 - 815.07.
8. Georgia: Ga. Code Ann. §§ 16-9-90 - 16-9-95.
9. Hawaii: Hawaii, Act 220-84.
10. Idaho: Idaho Code §§ 18-2201 - 18-2202, 26-1220.
11. Illinois: Ill. Ann. Stat. ch. 38 § 16-9.
12. Iowa: Iowa Code Ann. § 716A.1 - 716A.16.
13. Kentucky: Ky. Rev. Stat. §§ 434.550 - 434.715 (credit or debit cards), 434.840 - 434.860 (computer access).
14. Maryland: Maryland Ann. Code ch. 27 § 146.
15. Massachusetts: Mass. Gen. Laws Ann. ch. 266 § 30.
16. Michigan: M. S. A. §§ 28.529(1) - 28.529(7).
17. Minnesota: Minn. Stat. Ann. §§ 609.87 - 609.89.
18. Missouri: Mo. Ann. Stat. §§ 569.093 - 569.099.
19. Montana: Mont. Code Ann. §§ 45-1-205(2), 45-2-101(8) - 45-2-101(13), 45-2-101(54)(k), 45-2-101(69)(a)(iii), 45-6-310 - 45-6-311.
20. Nevada: Nev. Rev. Stat. §§ 205.473 - 205.477.
21. New Mexico: N.M. Stat. Ann. §§ 15-1A-13, 30-16A-1 - 30-16A-4.
22. North Carolina: N.C. Gen. Stat. §§ 14-453 - 14-457.
23. North Dakota: N.D. Century Code §§ 12.1-061-01, 12.1-06.1-08.
24. Ohio: Ohio Rev. Code Ann. §§ 2913.01 subsections (f) and (L) - (Q), 2913.43, 2901.01.
25. Oklahoma: Okla. Stat. §§ 21-1951 - 21-1956.
26. Pennsylvania: Pa. Stat. Ann. tit. 18 § 3933.
27. Rhode Island: R.I. Gen. Laws 11-52-1 through 11-52-4.
28. South Dakota: S.D. Cod. Laws §§ 43-43B-1 - 43-43B-8.
29. Tennessee: Tenn. Code Ann. §§ 39-3-1401 to 39-3-1406.
30. Utah: Utah Code Ann. §§ 76-6-701 - 76-6-704.
31. Virginia: Va. Code § 18.2-98.1.
32. Washington: Wash. Leg. Ser. ch. 273 (House Bill No. 1106, adopted March 28, 1984).
33. Wisconsin: Wis. Stat. Ann. § 943.70.
34. Wyoming: Wyo. Stat. Ann. §§ 6-3-501 - 6-3-505.

APPENDIX E

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

NSD Directive 145
(Unclassified Version)

THE WHITE HOUSE

WASHINGTON

September 17, 1984

National Security
Decision Directive 145
(Unclassified Version)

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems.

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems.

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest,

shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued.

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies.

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information.

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group.

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy

Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Director, National Security Agency
Manager, National Communications System

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order

12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman.

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year.

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments.

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives.

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems.

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechnical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems.

12. The functions of the Interagency Group for Telecommunications Protection and the National Communications Security Committee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively.

13. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled.

APPENDIX F

FEDERAL STATUTES PROVIDING PENALTIES FOR
UNLAWFULLY ACCESSING INFORMATION*

*Source: U.S. Department of Justice Bureau of Justice, Computer Crime, Legislative Resource.

Category A--Statutes Providing Criminal Penalties for Unlawfully Accessing Information

There are several key Federal statutes which provide criminal penalties for unlawfully obtaining information. Since information stored within a computer may be the target of the criminal act these provisions may be increasingly relevant. These include the following:

- Privacy Act (5 USC §552 a (i) (3)--The Privacy Act of 1974 governs the collection, maintenance, use and dissemination of individually-identifiable information contained in Federal agency records systems, and provides for access by an individual to his or her own records. The Act makes it a misdemeanor subject to a fine of not more than $5,000 for any person to knowingly and willfully request or obtain records under false pretenses. There have thus far been no criminal prosecutions under this or under either of the other two criminal penalty provisions of the Act.

- Embezzlement or Theft of Government Property (18 USC §641)--This statute provides criminal penalties for the embezzlement or theft of any record, voucher, money, or thing of value belonging to the United States, or thing made or being made under contract for the United States. The property in question must belong to the United States and the individual prosecuted must have had knowledge that it did. The Second Circuit has held that this statute is not limited in its coverage to tangible property, and is violated by the sale of information.[4]

- Espionage Act (18 USC §793 (a), (b), (c), (g))--Espionage Act provisions make unlawful specified activities undertaken for the purpose of obtaining information with respect to the national defense, and with an intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation. The term "national defense" in the context of these provisions has been interpreted as a generic concept of broad connotation.[5]

- Wire Fraud Statute (18 USC §1343)--This statute provides criminal penalties for fraudulently obtaining or attempting to obtain money or property through the use of wire, radio or television communications crossing State lines. The Fourth Circuit, on the facts of a recent case, held a computer system to be property within the meaning of this statute and affirmed a conviction under this statute for the fraudulent retrieval of information from a computer system without authorization.[6]

- Soliciting Federal tax information (26 USC § 7213 (a)(4))--This provision, amended to the Tax Code in 1978, subjects to criminal prosecution any person who willfully offers any item of material value in exchange for any tax return or tax return information, and who receives as a result of such solicitation any such return or return information. There have thus far been no reported prosecutions.

- Fair Credit Reporting Act (15 USC §1681 a)--This provision of the Fair Credit Reporting Act provides criminal penalties for obtaining information on a consumer from a reporting agency under false pretenses. The defendant must have acted knowingly and willfully. The Ninth Circuit has held that in addition to criminal prosecution, the statute permits a private suit by the individual on whom the information was unlawfully obtained.[7]

- Electronic Funds Transfer Act (15 USC §1693 n)--This provision of the Electronic Fund Transfers Act provides criminal penalties for various forms of misuse of any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument. The statute defines debit instrument as a card, code, or device, other than a check, draft or similar paper instrument, by the use of which a person may initiate an electronic funds transfer. The purpose of the Act as a whole is to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems; its primary objective is the provision of individual consumer rights.

Category B--Statutes Providing Criminal Penalties for Unlawfully Disclosing Information

The following Federal statutes provide a criminal penalty for unlawfully disclosing, as distinguished from obtaining, information. Such criminal sanctions may be applicable to acts by technical custodians of information (e.g., data processing personnel) or by other persons having indirect access to information stored in an automated environment.

- Privacy Act (5 USC §552 a (i)(1), (m), (b))--Paragraph (i)(1) of the Privacy Act makes it a misdemeanor subject to a fine of not more than $5,000 for a Federal agency officer or employee to knowingly and willfully disclose information except as permitted by the Act. Contractors, as defined in paragraph (m), are likewise subject to the Act's criminal penalties. The 11 specific conditions under which disclosure of information is permitted by the Act are delineated in paragraph (b). There have thus far been no criminal prosecutions under

this or either of the other two criminal penalty provisions of the Act.

- Disclosure of census data (13 USC §§9, 214)--This provision stipulates that no Commerce Department officer or employee may permit anyone other than the sworn officers and employees of the Department to examine any individual census report; it further stipulates that individual census reports shall be immune even from legal process. Contravention of this statute by present or former Commerce Department employees subjects them to criminal penalties under 13 USC §214.

- Espionage Act (18 USC §§793(d), (e), (f), (g), 794)--These provisions of the Espionage Act provide criminal penalties for specified acts of transmitting, losing, gathering or delivering national defense information with an intent to advantage a foreign nation or injure the United States. The information need not be classified.[8]

- Trade Secrets Act (18 USC §1905)--The Trade Secrets Act subjects officers and employees of the United States to fines of not more than $1,000 or imprisonment for not more than one year, or both, and to removal from office or employment, for any disclosure not authorized by law of trade secret information to which one is privy by virtue of his or her position. There have been no reported prosecutions under the Act. Additionally, it has been held that an individual or corporation has no right under the Act to initiate a private suit to prevent disclosures of information by Federal employees in violation of the Act.[9]

- Disclosing Federal tax return information (26 USC §7213(a))--This provision subjects the unlawful disclosure of tax returns and tax return information to fines of not more than $5,000, or imprisonment for not more than five years, or both, together with the costs of prosecution. (Regarding those instances where the disclosure of such information is authorized by law, see 21 USC §6103 and the section entitled Provisions Affording Access for Law Enforcement Purposes, below.)

- Redisclosure of privileged information (44 USC §3508)--This provision provides, in pertinent part, that if information obtained in confidence by a Federal agency is released by that agency to another Federal agency, all the provisions of law--including penalties which relate to the unlawful disclosure of information--apply to the officers and employees of the agency to which information is released, to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information.

- Fair Credit Reporting Act (15 USC §1681 (r), (s))--The Fair Credit Reporting Act, in subsection (r), stipulates that any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined not more than $5,000, or imprisoned for not more than one year, or both. Subsection (s) provides that enforcement shall be by the Federal Trade Commission.

- Disclosure of prepared income tax data (26 USC §7216)--This provision makes it a misdemeanor for an income tax preparer to disclose, except as otherwise authorized by law, information furnished to him or her in connection with the preparation of a Federal income tax return.

Category C--Provisions Impacting on Disclosure But Entailing No Criminal Penalties

The following Federal laws may impact on the disclosure of information (which could include computer data) but impose no criminal penalties.

- Confidentiality of child abuse records (42 USC §5103 (b) (2) (E))--This provision requires that, in order for a State to qualify for Federal financial assistance in developing, strengthening, and carrying out child abuse and neglect prevention and treatment programs, the State must provide for methods to preserve the confidentiality of all records so as to protect the rights of children, and their parents or guardians.

- Disclosure of classified information (E.O. 12065)--Except as provided in the Atomic Energy Act of 1954, as amended, this Executive Order constitutes the sole standard and basis for classifying information. Section 5-5 of the Order provides for administrative sanctions. Federal Government officers and employees shall be subject to such sanctions for knowing and willfull violation of any provision of the Order, including classifying information in violation of the Order, or for disclosing without authorization, properly classified information. Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, or any other sanction in accordance with applicable law and agency regulations.

- Right to Financial Privacy Act (12 USC §3401 et seq.)--Section 3417 of the Right to Financial Privacy Act provides that any agency or department of the United States or financial institution obtaining or disclosing financial records of information contained therein in viola-

tion of the Act shall be liable to the customer to whom such records relate. It also provides in certain instances for disciplinary action against Federal Government officers or employees so involved. Section 3418 provides that a customer may also seek an injunction to require that the procedures of the Act are complied with.

- Family Educational Rights and Privacy Act (20 USC §1232 g)--The Family Educational Rights and Privacy Act conditions Federal funding of educational institutions and agencies on (1) their permitting parents of students access to the educational records of their children, and (2) their otherwise limiting access to such records to those specified in the Act. Enforcement of this provision is solely in the hands of the Secretary of Education; no private remedy is granted under the statute.[11]

- Disclosure of Federal income tax return (26 USC §7217)--By this provision, a taxpayer may bring a civil action for damages in Federal court against any person who knowingly or negligently has disclosed that taxpayer's tax return or return informaiton, other than as authorized or in good faith understood to be authorized by 26 USC §6103.

Category D--Provisions Requiring Safeguarding of Information

The following Federal statutes require that certain information be safeguarded and may be of possible applicability to computer related crime cases.

- Privacy Act (5 USC §552 a (e) (10))--The Privacy Act of 1974, in one of several agency requirements enumerated in paragraph (e), stipulates that an agency that maintains a system of records shall establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. (Paragraph (e) (10).

- Tax Reform Act of 1976 (26 USC §6103 (p)(4-8))--These provisions of the Tax Reform Act of 1976 require that any Federal agency, body, or commission and the General Accounting Office, as a condition for receiving tax returns or return information, provide safeguards for the confidentiality of such information, to the satisfaction of the Secretary of the Treasury. The provisions similarly require that States adopt provisions of law to safeguard Federal tax return information.

- Safeguarding against unauthorized removal or destruction of records (44 USC §§3105, 3106)--These provisions require, among other things, the establishment by Federal agencies of safeguards against the removal or loss of necessary records (§3105) and notification to the Administrator of the General Services Administration and, when appropriate, to the Attorney General in case of actual or forseeable unlawful removal or destruction of records (§3106).

- Classification of information (E.O.10865)--This Executive Order, in pertinent part, provides that the heads of agencies designated in the Order prescribe regulations for the safeguarding of classified information within key industries. The Order states that such regulations shall, so far as possible, be uniform and provide for full cooperation among the agencies concerned.

- Controlling access to classified information (E.O. 12065 §4)--Section 4 of this Executive Order provides for the safeguarding and, in particular, the controlling of access to classified information.

Category E--Statutory Provisions Allowing Access for Law Enforcement Purposes Only

Several provisions of Federal law allow access to otherwise confidential information by law enforcement. These may be relevant in connection with the detection and/or prosecution of computer related crimes.

- Exceptions under Privacy Act USC §552)--The Privacy Act of 1974's provision that information not be disclosed without the written consent of the individual affected is subject to 11 exceptions. These include disclosure (1) for a routine use [12] [a use compatible with the purpose for which the information was collected; routine uses are required to be specified in the Federal Register], (2) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the U.S. for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought,[13] and (3) pursuant to the order of a court of competent jurisdiction.[14]

- Disclosure of Federal tax information (26 USC §6103)--This provision in paragraphs (c) through (o) delineates

the persons to whom, and the purposes for which and conditions under which tax returns and return information may be disclosed. Pertinent to this chapter are paragraphs (h) and (i), which concern disclosures to Federal officers and employees (including those of the Department of Justice), for, respectively, purposes of tax administration and the administration of Federal laws not relating to tax administration.

- Disclosure of otherwise classified information (E.O. 12065)--Section 5-505 of this Executive Order requires that agency heads report to the Attorney General any evidence reflected in classified information of possible violations of Federal criminal law by an agency employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General.

- Disclosure of bank records (12 USC §3401 et seq.)--The Right to Financial Privacy Act provides that bank records may be obtained by Government authorities, but only in accordance with one of five specified procedures--customer authorization, administrative subpoena, judicial subpoena, formal written request, or search warrant. The Act sets forth the necessary conditions and procedures for each, including the manner in which notice and a right to be heard are to be afforded the depositor with each of the first four.[15]

- Disclosure of consumer credit information (15 USC §1681)--The Fair Credit Reporting Act provides in Subsection b(1) that a consumer reporting agency may furnish to a Government agency identifying information with respect to any consumer, limited to his name, address, former addresses, places of employment, or former places of employment.[16]

- Judicial order for educational records (20 USC §1232 g)--Among the limited and specified exceptions to the confidentiality of educational records provided for in the Family Educational Rights and Privacy Act is an exception under 20 USC §1232 g (b)(2)(B) for information furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency.[17]

- Investigatory Records under Freedom of Information Act (5 USC §552)--The Freedom of Information Act requires that Federal agency records be made available to any person making a proper request. However, the Act specifies nine categories of records which may be withheld at the reasonable discretion of an agency. One of these

nine is "investigatory records compiled for law enforcement purposes".[18] These can be withheld only to the extent that production of such records would (a) interfere with enforcement proceedings,[19] (b) deprive a person of a right to a fair trial or an impartial adjudication, (c) constitute an unwarranted invasion of personal privacy,[20] (d) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, disclose confidential information furnished only by the confidential source,[21] (e) disclose investigative techniques or procedures, or (f) endanger the life or physical safety of law enforcement personnel."

STATE STATUTES PROVIDING FOR CONFIDENTIALITY OF COMPUTERIZABLE INFORMATION

A total of 44 of the 50 States have statutes on their books which provide for the confidentiality of one or more categories of computerizable information. In all, over 150 such statutes exist. Table 2.2, below, indicates the eight major groups into which such statutes fall and the number of statutes which research suggests fall in each group nationwide, as of the time of this writing.

CONCLUSIONS

The concern in informational privacy law is not specifically computers, but information. While the treatment of informational privacy law herein has been limited to provisions affecting computerizable information, the scope of these provisions extends generally to all forms of information--whether or not computerized. Where information is maintained on computers, these provisions may be relevant to the investigation and/or prosecution of computer related crime in one or another of several ways. As we have seen, certain provisions may be relevant to prosecution in that they provide criminal penalties for unlawfully obtaining or disclosing information. Other provisions may be relevant to both investigation and prosecution in that they afford access for law enforcement purposes to otherwise unavailable information or they afford control for law enforcement purposes over otherwise available information. Certain other important disclosure-prohibiting provisions have also been included though they entail no criminal penalties.

APPENDIX G

AMERICAN BAR ASSOCIATION REPORT ON COMPUTER CRIME SUMMARY OF FINDINGS

APPENDIX G

A summary of the survey findings include the following:

1. The most significant types of computer crime, according to the respondents, are:

   -- Use of computers to steal tangible or intangible assets

   -- Destruction or alteration of data

   -- Use of computers to embezzle funds

   -- Destruction or alteration of software

   - Use of computers to defraud consumers, investors or users

2. Computer crime is regarded by the survey respondents as less important than most violent crimes, but of equal or greater importance than many other types of White Collar Crime, including antitrust violations, counterfeiting, consumer fraud, bank fraud and embezzlement, securites fraud, and tax fraud.

3. The annual losses incurred as a result of computer crime appear, by any measure, to be enormous. Over 25% (72)of the survey repsondents reported "known and verifiable losses due to computer crime during the last twelve months." The total annual losses reported by these respondents fall somewhere between $145 million and $730 million. Thus, the annual losses per respondent reporting losses could be anywhere from $2 million to as high as $10 million. Approximately 28% of the survey respondents reported no available system to monitor or estimate the value of their computer crime losses.

4. Approximately 48% (136) of the survey reposndents reported that they had experienced "known and verifiable incidents of computer crime" during the past twelve months. the most frequently mentioned incidents were those involving: (1) unauthorized use of business computers for personal activities; 2) theft of computer software; 3) theft of tangible or intangible assets by means of a computer; 4) theft of computer hardware; and 5) destruction or alteration of software and/or data.

5. A large proportion of the reponsdents (39%) indicated that they had not been able to identify the perpetrators of known incidents of computer crime. Of the perpetrators identified, 78% of the respondents (125) indicated that the perpetrators were individuals within their organization; 46% (73) indicated that the identified perpetrators were individuals outside the organization.

6. Of the 148 respondents indicating that they had experienced incidents of computer crime (not necessarily during the past twelve months), approximately one-third reported that none of the incidents had been reported to law enforcement authorities, and another one-third reported that only some of the incidents had been reported. The remaining respondents indicated that most or all such incidents had been reported.

7. The respondents were asked to rank various means of preventing and deterring computer crime in terms of their effectiveness. the top-ranked items were as follows: 1) more comprehensive and effective self protection by private business; 2) education of users concerning vulnerabilities of computer usage; 3) more severe penalties in federal and state criminal statutes; and 4) greater education of the public regarding computer crime.

8. The respondents were then asked to identify the steps that their organizations have actually taken to prevent and determine computer crime. The most frequently mentioned self-protection steps were: 1) limited access to computer programs, computer logic (85%); 2) limited access to computer operations (81%); 3) frequent changing of access codes, user ID numbers (72%); 4) limited access to input of data into computer (71%); 5) installation of asset controls and accountability (57%); 6) frequent security checks of computer and operations (50%); and 7) security education for employees (49%). the least-mentioned protective steps were prompt referral of suspected illegal activity to law enforcement authorities (20%), and coding of input or output data (14%).

9. The respondents were asked their views regarding the need for a federal criminal statute directed specifically to computer crime. their views were as follows: strongly support -163 (58%); somewhat support = 58 (21%); no opinion = 43 (15%); somewhat oppose = 12 (4%); strongly oppose = 4 (1%).

10. The respondents were asked to provide written comments concerning "the most troublesome current and future aspects of computer crime." Over 60% (175) of the respondents provided such comments. The concerns most often articulated were the following: 1) the proliferation of business and personal computers and computer users; 2) the difficulty of detecting computer crime; 3) the existing vulnerability to computer crime, lack of adequate security measures; 4) the lack of public and/or managerial awareness and concern; and 5) the growing magnitude of potential losses from computer crime. Furthermore the task force viewed these findings as an initial step and planned to provide additional recommendations in a future report.

DISTRIBUTION LIST FOR P-1798

Distribution List for P-1798

DEPARTMENT OF DEFENSE

Honorable Donald C. Latham
Assistant Secretary of Defense
C3I Pentagon, Room 3E172
Washington, D.C. 20301

Col. John Lane
Director, Information Systems
Assistant Secretary of Defense C3I
Pentagon, Room 3E187
Washington, D.C. 20301

Major Susan Swift
Military Assistant Information Systems
Assistant Secretary of Defense,
C3I Pentagon, Room 3E187
Washington, D.C. 20301

Lt. General Lincoln D. Faurer
Director National Security Agency
Fort George Meade, Maryland 20755

Walter Deeley
Deputy Director Communications Security
National Security Agency
Fort George Meade, Maryland 20755

Robert K. Little
Assistant Director of
Resources and Systems
Defense Intelligence Agency
Pentagon, Room 3E286
Washington, D.C. 20301

Honorable Joseph H. Sherick
The Inspector General
Department of Defense
Pentagon, Room 1E482
Washington, D.C. 20301

Michael C. Eberhardt
Assistant Inspector General
Criminal Investigations Oversight Policy
Commonwealth Building
1300 Wilson Blvd
Arlington, Virginia 22209

John Springitt
Department of Defense
Comptroller
Information Resources Management Directorate
Pentagon Room 3A336
Washington, D.C. 20301

General John W. Vessey, Jr.
Chairman, Joint Chiefs of Staff
The Pentagon, Room 3E873
Washington, D.C. 20301

Honorable John O. Marsh, Jr.
Secretary of the Army
The Pentagon, Room 3E178
Washington, D.C. 20301

Honorable John F. Lehman, Jr.
Secretary of the Navy
The Pentagon, Room 4E686
Washington, D.C. 20301

Honorable Verne Orr
Secretary of the Air Force
The Pentagon, Room 4E874
Washington, D.C. 20301

Mr. James H. Miller
OASD/MI&L (PI)
The Pentagon, Room 3C800
Washington, D.C. 20301

FEDERAL GOVERNMENT, CONTRACTORS, AND OTHERS

Dr. Dennis Branstad
Institute for Computer Science and Technology
National Bureau of Standards
Administration Building
Gaithersburg, Maryland 20760

Joesph Wright, Jr.
Deputy Director
Office of Management and Budget
Old Executive Office Building
17th and Pennsylvania N.W.
Washington, D.C. 20503

Lee Colwell
Executive Assistant Director
Federal Bureau of Investigation
J. Edgar Hoover Building
9th and Pennsylvania Ave. N.W.
Washington, D.C. 20535

William A. Bayse
Assistant Director, Technical Div.
Federal Bureau of Investigation
J. Edgar Hoover Building
9th and Pennsylvania Ave. N.W.
Washington, D.C. 20535

Robert E. Conley
Acting Assistant Secretary for Electronic
Systems and Information Technology
Department of Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

David Bailey
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Alexander D. Roth
Abrams, Westermeier and Goldberg, P.C.
1828 L Street N.W.
Washington, D.C. 20036

Toni Carbo Bearman
Executive Director
National Commission on Libraries and
Information Science
Suite 601
1717 K Street, N.W.
Washington, D.C. 20036

Walter Anderson
Information Management Technology
U.S. General Accounting Office
441 G Street N.W.
Washington, D.C. 20548

DoD - IDA Management Office
1801 N. Beauregard St.
Alexandria, VA 22311

Defense Technical Information Center (2 copies)
Cameron Station
Alexandria, VA 22314

CSED REVIEW PANEL

Dr. Dan Alpert
Director, Center for Advanced Study
University of Illinois
912 W. Illinois Street
Urbana, IL 61801

Dr. Barry W. Boehm
TRW Defense Systems Group
MS 02-2304
One Space Park
Redondo Beach, CA 90278

Dr. Ruth Davis
The Pymatuning Group, Inc.
2000 L Street, N.W.,
Suite 702
Washington, D.C. 20036

Dr. Larry E. Druffel
Rational Machines
1501 Salado Drive
Mountain View, CA 94043

Mr. Neil S. Eastman
Manager, Software Engineering & Technology
IBM Federal Systems Division
6600 Rockledge Drive
Bethesda, MD 20817

Dr. Charles E. Hutchinson
Dean, Thayer School of Engineering
Dartmouth College
Hanover, NH 03755

Mr. Oliver Selfridge
45 Percy Road
Lexington, MA 02173

IDA

Mr. Deitchman
Mr. Pirie
Mr. Van Atta
Dr. Probert
Dr. Kramer
Dr. Slusarczuk
Ms. Becker (75 copies)
Ms. Powell
Mr. Campbell
Ms. Lyons
Mr. Higgins

END

FILMED

2-85

DTIC